

Finite Group Theory

I. Martin Isaacs

**Graduate Studies
in Mathematics**

Volume 92



American Mathematical Society

Finite Group Theory

I. Martin Isaacs

Graduate Studies
in Mathematics

Volume 92



American Mathematical Society
Providence, Rhode Island

Editorial Board

David Cox (Chair)

Steven G. Krantz

Rafe Mazzeo

Martin Scharlemann

2000 *Mathematics Subject Classification*. Primary 20B15, 20B20, 20D06, 20D10, 20D15, 20D20, 20D25, 20D35, 20D45, 20E22, 20E36.

For additional information and updates on this book, visit
www.ams.org/bookpages/gsm-92

Library of Congress Cataloging-in-Publication Data

Isaacs, I. Martin, 1940–

Finite group theory / I. Martin Isaacs.

p. cm. — (Graduate studies in mathematics ; v. 92)

Includes index.

ISBN 978-0-8218-4344-4 (alk. paper)

1. Finite groups. 2. Group theory. I. Title.

QA177.I835 2008

512'.23—dc22

2008011388

Copying and reprinting. Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

© 2008 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 13 12 11 10 09 08

To Deborah

Contents

Preface	ix
Chapter 1. Sylow Theory	1
Chapter 2. Subnormality	45
Chapter 3. Split Extensions	65
Chapter 4. Commutators	113
Chapter 5. Transfer	147
Chapter 6. Frobenius Actions	177
Chapter 7. The Thompson Subgroup	201
Chapter 8. Permutation Groups	223
Chapter 9. More on Subnormality	271
Chapter 10. More Transfer Theory	295
Appendix: The Basics	325
Index	345

Preface

This book is a somewhat expanded version of a graduate course in finite group theory that I often teach at the University of Wisconsin. I offer this course in order to share what I consider to be a beautiful subject with as many people as possible, and also to provide the solid background in pure group theory that my doctoral students need to carry out their thesis work in representation theory.

The focus of group theory research has changed profoundly in recent decades. Starting near the beginning of the 20th century with the work of W. Burnside, the major problem was to find and classify the finite simple groups, and indeed, many of the most significant results in pure group theory and in representation theory were directly, or at least peripherally, related to this goal. The simple-group classification now appears to be complete, and current research has shifted to other aspects of finite group theory including permutation groups, p -groups and especially, representation theory.

It is certainly no less essential in this post-classification period that group-theory researchers, whatever their subspecialty, should have a mastery of the classical techniques and results, and so without attempting to be encyclopedic, I have included much of that material here. But my choice of topics was largely determined by my primary goal in writing this book, which was to convey to readers my feeling for the beauty and elegance of finite group theory.

Given its origin, this book should certainly be suitable as a text for a graduate course like mine. But I have tried to write it so that readers would also be comfortable using it for independent study, and for that reason, I have tried to preserve some of the informal flavor of my classroom. I have tried to keep the proofs as short and clean as possible, but without omitting

details, and indeed, in some of the more difficult material, my arguments are simpler than can be found in print elsewhere. Finally, since I firmly believe that one cannot learn mathematics without doing it, I have included a large number of problems, many of which are far from routine.

Some of the material here has rarely, if ever, appeared previously in books. Just in the first few chapters, for example, we offer Zenkov's marvelous theorem about intersections of abelian subgroups, Wielandt's "zipper lemma" in subnormality theory and a proof of Horosevskii's theorem that the order of a group automorphism can never exceed the order of the group. Later chapters include many more advanced topics that are hard or impossible to find elsewhere.

Most of the students who attend my group-theory course are second-year graduate students, with a substantial minority of first-year students, and an occasional well-prepared undergraduate. Almost all of these people had previously been exposed to a standard first-year graduate abstract algebra course covering the basics of groups, rings and fields. I expect that most readers of this book will have a similar background, and so I have decided not to begin at the beginning.

Most of my readers (like my students) will have previously seen basic group theory, so I wanted to avoid repeating that material and to start with something more exciting: Sylow theory. But I recognize that my audience is not homogeneous, and some readers will have gaps in their preparation, so I have included an appendix that contains most of the assumed material in a fairly condensed form. On the other hand, I expect that many in my audience will already know the Sylow theorems, but I am confident that even these well-prepared readers will find material that is new to them within the first few sections.

My semester-long graduate course at Wisconsin covers most of the first seven chapters of this book, starting with the Sylow theorems and culminating with a purely group-theoretic proof of Burnside's famous $p^a q^b$ -theorem. Some of the topics along the way are subnormality theory, the Schur-Zassenhaus theorem, transfer theory, coprime group actions, Frobenius groups, and the normal p -complement theorems of Frobenius and of Thompson. The last three chapters cover material for which I never have time in class. Chapter 8 includes a proof of the simplicity of the groups $PSL(n, q)$, and also some graph-theoretic techniques for studying subdegrees of primitive and nonprimitive permutation groups. Subnormality theory is revisited in Chapter 9, which includes Wielandt's beautiful automorphism tower theorem and the Thompson-Wielandt theorem related to the Sims

conjecture. Finally, Chapter 10 presents some advanced topics in transfer theory, including Yoshida's theorem and the so-called "principal ideal theorem".

Finally, I thank my many students and colleagues who have contributed ideas, suggestions and corrections while this book was being written. In particular, I mention that the comments of Yakov Berkovich and Gabriel Navarro were invaluable and very much appreciated.

Sylow Theory

1A

It seems appropriate to begin this book with a topic that underlies virtually all of finite group theory: the Sylow theorems. In this chapter, we state and prove these theorems, and we present some applications and related results. Although much of this material should be very familiar, we suspect that most readers will find that at least some of the content of this chapter is new to them.

Although the theorem that proves Sylow subgroups always exist dates back to 1872, the existence proof that we have decided to present is that of H. Wielandt, published in 1959. Wielandt's proof is slick and short, but it does have some drawbacks. It is based on a trick that seems to have no other application, and the proof is not really constructive; it gives no guidance about how, in practice, one might actually find a Sylow subgroup. But Wielandt's proof is beautiful, and that is the principal motivation for presenting it here.

Also, Wielandt's proof gives us an excuse to present a quick review of the theory of group actions, which are nearly as ubiquitous in the study of finite groups as are the Sylow theorems themselves. We devote the rest of this section to the relevant definitions and basic facts about actions, although we omit some details from the proofs.

Let G be a group, and let Ω be a nonempty set. (We will often refer to the elements of Ω as “points”.) Suppose we have a rule that determines a new element of Ω , denoted $\alpha \cdot g$, whenever we are given a point $\alpha \in \Omega$ and an element $g \in G$. We say that this rule defines an **action** of G on Ω if the following two conditions hold.

- (1) $\alpha \cdot 1 = \alpha$ for all $\alpha \in \Omega$ and
- (2) $(\alpha \cdot g) \cdot h = \alpha \cdot (gh)$ for all $\alpha \in \Omega$ and all group elements $g, h \in G$.

Suppose that G acts on Ω . It is easy to see that if $g \in G$ is arbitrary, then the function $\sigma_g : \Omega \rightarrow \Omega$ defined by $(\alpha)\sigma_g = \alpha \cdot g$ has an inverse: the function $\sigma_{g^{-1}}$. Therefore, σ_g is a permutation of the set Ω , which means that σ_g is both injective and surjective, and thus σ_g lies in the symmetric group $\text{Sym}(\Omega)$ consisting of all permutations of Ω . In fact, the map $g \mapsto \sigma_g$ is easily seen to be a homomorphism from G into $\text{Sym}(\Omega)$. (A homomorphism like this, which arises from an action of a group G on some set, is called a **permutation representation** of G .) The kernel of this homomorphism is, of course, a normal subgroup of G , which is referred to as the **kernel** of the action. The kernel is exactly the set of elements $g \in G$ that act trivially on Ω , which means that $\alpha \cdot g = \alpha$ for all points $\alpha \in \Omega$.

Generally, we consider a theorem or a technique that has the power to find a normal subgroup of G to be “good”, and indeed permutation representations can be good in this sense. (See the problems at the end of this section.) But our goal in introducing group actions here is not to find normal subgroups; it is to count things. Before we proceed in that direction, however, it seems appropriate to mention a few examples.

Let G be arbitrary, and take $\Omega = G$. We can let G act on G by right multiplication, so that $x \cdot g = xg$ for $x, g \in G$. This is the **regular** action of G , and it should be clear that it is **faithful**, which means that its kernel is trivial. It follows that the corresponding permutation representation of G is an isomorphism of G into $\text{Sym}(G)$, and this proves Cayley’s theorem: every group is isomorphic to a group of permutations on some set.

We continue to take $\Omega = G$, but this time, we define $x \cdot g = g^{-1}xg$. (The standard notation for $g^{-1}xg$ is x^g .) It is trivial to check that $x^1 = x$ and that $(x^g)^h = x^{gh}$ for all $x, g, h \in G$, and thus we truly have an action, which is called the **conjugation** action of G on itself. Note that $x^g = x$ if and only if $xg = gx$, and thus the kernel of the conjugation action is the set of elements $g \in G$ that commute with all elements $x \in G$. The kernel, therefore, is the center $\mathbf{Z}(G)$.

Again let G be arbitrary. In each of the previous examples, we took $\Omega = G$, but we also get interesting actions if instead we take Ω to be the set of all subsets of G . In the conjugation action of G on Ω we let $X \cdot g = X^g = \{x^g \mid x \in X\}$ and in the right-multiplication action we define $X \cdot g = Xg = \{xg \mid x \in X\}$. Of course, in order to make these examples work, we do not really need Ω to be *all* subsets of G . For example, since a conjugate of a subgroup is always a subgroup, the conjugation action is well defined if we take Ω to be the set of all subgroups of G . Also, both right multiplication

and conjugation preserve cardinality, and so each of these actions makes sense if we take Ω to be the collection of all subsets of G of some fixed size. In fact, as we shall see, the trick in Wielandt's proof of the Sylow existence theorem is to use the right multiplication action of G on its set of subsets with a certain fixed cardinality.

We mention one other example, which is a special case of the right-multiplication action on subsets that we discussed in the previous paragraph. Let $H \subseteq G$ be a subgroup, and let $\Omega = \{Hx \mid x \in G\}$, the set of right cosets of H in G . If X is any right coset of H , it is easy to see that Xg is also a right coset of H . (Indeed, if $X = Hx$, then $Xg = H(xg)$.) Then G acts on the set Ω by right multiplication.

In general, if a group G acts on some set Ω and $\alpha \in \Omega$, we write $G_\alpha = \{g \in G \mid \alpha \cdot g = \alpha\}$. It is easy to check that G_α is a subgroup of G ; it is called the **stabilizer** of the point α . For example, in the regular action of G on itself, the stabilizer of every point (element of G) is the trivial subgroup. In the conjugation action of G on G , the stabilizer of $x \in G$ is the centralizer $C_G(x)$ and in the conjugation action of G on subsets, the stabilizer of a subset X is the normalizer $N_G(X)$. A useful general fact about point stabilizers is the following, which is easy to prove. In any action, if $\alpha \cdot g = \beta$, then the stabilizers G_α and G_β are conjugate in G , and in fact, $(G_\alpha)^g = G_\beta$.

Now consider the action (by right multiplication) of G on the right cosets of H , where $H \subseteq G$ is a subgroup. The stabilizer of the coset Hx is the set of all group elements g such that $Hxg = Hx$. It is easy to see that g satisfies this condition if and only if $xg \in Hx$. (This is because two cosets Hu and Hv are identical if and only if $u \in Hv$.) It follows that g stabilizes Hx if and only if $g \in x^{-1}Hx$. Since $x^{-1}Hx = H^x$, we see that the stabilizer of the point (coset) Hx is exactly the subgroup H^x , conjugate to H via x . It follows that the kernel of the action of G on the right cosets of H in G is exactly $\bigcap_{x \in G} H^x$. This subgroup is called the **core** of H in G , denoted $\text{core}_G(H)$. The core of H is normal in G because it is the kernel of an action, and, clearly, it is contained in H . In fact, if $N \triangleleft G$ is any normal subgroup that happens to be contained in H , then $N = N^x \subseteq H^x$ for all $x \in G$, and thus $N \subseteq \text{core}_G(H)$. In other words, the core of H in G is the unique largest normal subgroup of G contained in H . (It is "largest" in the strong sense that it contains all others.)

We have digressed from our goal, which is to show how to use group actions to count things. But having come this far, we may as well state the results that our discussion has essentially proved. Note that the following theorem and its corollaries can be used to prove the existence of normal subgroups, and so they might be considered to be "good" results.

1.1. Theorem. *Let $H \subseteq G$ be a subgroup, and let Ω be the set of right cosets of H in G . Then $G/\text{core}_G(H)$ is isomorphic to a subgroup of $\text{Sym}(\Omega)$. In particular, if the index $|G : H| = n$, then $G/\text{core}_G(H)$ is isomorphic to a subgroup of S_n , the symmetric group on n symbols.*

Proof. The action of G on the set Ω by right multiplication defines a homomorphism θ (the permutation representation) from G into $\text{Sym}(\Omega)$. Since $\ker(\theta) = \text{core}_G(H)$, it follows by the homomorphism theorem that $G/\text{core}_G(H) \cong \theta(G)$, which is a subgroup of $\text{Sym}(\Omega)$. The last statement follows since if $|G : H| = n$, then (by definition of the index) $|\Omega| = n$, and thus $\text{Sym}(\Omega) \cong S_n$. ■

1.2. Corollary. *Let G be a group, and suppose that $H \subseteq G$ is a subgroup with $|G : H| = n$. Then H contains a normal subgroup N of G such that $|G : N|$ divides $n!$.*

Proof. Take $N = \text{core}_G(H)$. Then G/N is isomorphic to a subgroup of the symmetric group S_n , and so by Lagrange's theorem, $|G/N|$ divides $|S_n| = n!$. ■

1.3. Corollary. *Let G be simple and contain a subgroup of index $n > 1$. Then $|G|$ divides $n!$.*

Proof. The normal subgroup N of the previous corollary is contained in H , and hence it is proper in G because $n > 1$. Since G is simple, $N = 1$, and thus $|G| = |G/N|$ divides $n!$. ■

In order to pursue our main goal, which is counting, we need to discuss the “orbits” of an action. Suppose that G acts on Ω , and let $\alpha \in \Omega$. The set $\mathcal{O}_\alpha = \{\alpha \cdot g \mid g \in G\}$ is called the **orbit** of α under the given action. It is routine to check that if $\beta \in \mathcal{O}_\alpha$, then $\mathcal{O}_\beta = \mathcal{O}_\alpha$, and it follows that distinct orbits are actually disjoint. Also, since every point is in at least one orbit, it follows that the orbits of the action of G on Ω partition Ω . In particular, if Ω is finite, we see that $|\Omega| = \sum |\mathcal{O}|$, where in this sum, \mathcal{O} runs over the full set of G -orbits on Ω .

We mention some examples of orbits and orbit decompositions. First, if $H \subseteq G$ is a subgroup, we can let H act on G by right multiplication. It is easy to see that the orbits of this action are exactly the left cosets of H in G . (We leave to the reader the problem of realizing the right cosets of H in G as the orbits of an appropriate action of H . But be careful: the rule $x \cdot h = hx$ does *not* define an action.)

Perhaps it is more interesting to consider the conjugation action of G on itself, where the orbits are exactly the conjugacy classes of G . The fact

that for a finite group, the order $|G|$ is the sum of the sizes of the classes is sometimes called the **class equation** of G .

How big is an orbit? The key result here is the following.

1.4. Theorem (The Fundamental Counting Principle). *Let G act on Ω , and suppose that \mathcal{O} is one of the orbits. Let $\alpha \in \mathcal{O}$, and write $H = G_\alpha$, the stabilizer of α . Let $\Lambda = \{Hx \mid x \in G\}$ be the set of right cosets of H in G . Then there is a bijection $\theta : \Lambda \rightarrow \mathcal{O}$ such that $\theta(Hg) = \alpha \cdot g$. In particular, $|\mathcal{O}| = |G : G_\alpha|$.*

Proof. We observe first that if $Hx = Hy$, then $\alpha \cdot x = \alpha \cdot y$. To see why this is so, observe that we can write $y = hx$ for some element $h \in H$. Then

$$\alpha \cdot y = \alpha \cdot (hx) = (\alpha \cdot h) \cdot x = \alpha \cdot x,$$

where the last equality holds because $h \in H = G_\alpha$, and so h stabilizes α .

Given a coset $Hx \in \Lambda$, the point $\alpha \cdot x$ lies in \mathcal{O} , and we know that it is determined by the coset Hx , and not just by the particular element x . It is therefore permissible to define the function $\theta : \Lambda \rightarrow \mathcal{O}$ by $\theta(Hx) = \alpha \cdot x$, and it remains to show that θ is both injective and surjective.

The surjectivity is easy, and we do that first. If $\beta \in \mathcal{O}$, then by the definition of an orbit, we have $\beta = \alpha \cdot x$ for some element $x \in G$. Then $Hx \in \Lambda$ satisfies $\theta(Hx) = \alpha \cdot x = \beta$, as required.

To prove that θ is injective, suppose that $\theta(Hx) = \theta(Hy)$. We have $\alpha \cdot x = \alpha \cdot y$, and hence

$$\alpha = \alpha \cdot 1 = (\alpha \cdot x) \cdot x^{-1} = (\alpha \cdot y) \cdot x^{-1} = \alpha \cdot (yx^{-1}).$$

Then yx^{-1} fixes α , and so it lies in $G_\alpha = H$. It follows that $y \in Hx$, and thus $Hy = Hx$. This proves that θ is injective, as required. ■

It is easy to check that the bijection θ of the previous theorem actually defines a “permutation isomorphism” between the action of G on Λ and the action of G on the orbit \mathcal{O} . Formally, this means that $\theta(X \cdot g) = \theta(X) \cdot g$ for all “points” X in Λ and group elements $g \in G$. More informally, this says that the actions of G on Λ and on \mathcal{O} are “essentially the same”. Since every action can be thought of as composed of the actions on the individual orbits, and each of these actions is permutation isomorphic to the right-multiplication action of G on the right cosets of some subgroup, we see that these actions on cosets are truly fundamental: every group action can be viewed as being composed of actions on right cosets of various subgroups.

We close this section with two familiar and useful applications of the fundamental counting principle.

1.5. Corollary. Let $x \in G$, where G is a finite group, and let K be the conjugacy class of G containing x . Then $|K| = |G : \mathbf{C}_G(x)|$.

Proof. The class of x is the orbit of x under the conjugation action of G on itself, and the stabilizer of x in this action is the centralizer $\mathbf{C}_G(x)$. Thus $|K| = |G : \mathbf{C}_G(x)|$, as required. ■

1.6. Corollary. Let $H \subseteq G$ be a subgroup, where G is finite. Then the total number of distinct conjugates of H in G , counting H itself, is $|G : \mathbf{N}_G(H)|$.

Proof. The conjugates of H form an orbit under the conjugation action of G on the set of subsets of G . The normalizer $\mathbf{N}_G(H)$ is the stabilizer of H in this action, and thus the orbit size is $|G : \mathbf{N}_G(H)|$, as wanted. ■

Problems 1A

1A.1. Let H be a subgroup of prime index p in the finite group G , and suppose that no prime smaller than p divides $|G|$. Prove that $H \triangleleft G$.

1A.2. Given subgroups $H, K \subseteq G$ and an element $g \in G$, the set $HgK = \{h g k \mid h \in H, k \in K\}$ is called an (H, K) -double coset. In the case where H and K are finite, show that $|HgK| = |H||K|/|H \cap H^g|$.

Hint. Observe that HgK is a union of right cosets of H , and that these cosets form an orbit under the action of K .

Note. If we take $g = 1$ in this problem, the result is the familiar formula $|HK| = |H||K|/|H \cap K|$.

1A.3. Suppose that G is finite and that $H, K \subseteq G$ are subgroups.

- (a) Show that $|H : H \cap K| \leq |G : K|$, with equality if and only if $HK = G$.
- (b) If $|G : H|$ and $|G : K|$ are coprime, show that $HK = G$.

Note. Proofs of these useful facts appear in the appendix, but we suggest that readers try to find their own arguments. Also, recall that the product HK of subgroups H and K is not always a subgroup. In fact, HK is a subgroup if and only if $HK = KH$. (This too is proved in the appendix.) If $HK = KH$, we say that H and K are **permutable**.

1A.4. Suppose that $G = HK$, where H and K are subgroups. Show that also $G = H^x K^y$ for all elements $x, y \in G$. Deduce that if $G = HH^x$ for a subgroup H and an element $x \in G$, then $H = G$.

1A.5. An action of a group G on a set Ω is **transitive** if Ω consists of a single orbit. Equivalently, G is transitive on Ω if for every choice of points $\alpha, \beta \in \Omega$, there exists an element $g \in G$ such that $\alpha \cdot g = \beta$. Now assume that a group G acts transitively on each of two sets Ω and Λ . Prove that the natural induced action of G on the cartesian product $\Omega \times \Lambda$ is transitive if and only if $G_\alpha G_\beta = G$ for some choice of $\alpha \in \Omega$ and $\beta \in \Lambda$.

Hint. Show that if $G_\alpha G_\beta = G$ for some $\alpha \in \Omega$ and $\beta \in \Lambda$, then in fact, this holds for all $\alpha \in \Omega$ and $\beta \in \Lambda$.

1A.6. Let G act on Ω , where both G and Ω are finite. For each element $g \in G$, write $\chi(g) = |\{\alpha \in \Omega \mid \alpha \cdot g = \alpha\}|$. The nonnegative-integer-valued function χ is called the **permutation character** associated with the action. Show that

$$\sum_{g \in G} \chi(g) = \sum_{\alpha \in \Omega} |G_\alpha| = n|G|,$$

where n is the number of orbits of G on Ω .

Note. Thus the number of orbits is

$$n = \frac{1}{|G|} \sum_{g \in G} \chi(g),$$

which is the average value of χ over the group. Although this orbit-counting formula is often attributed to W. Burnside, it should (according to P. Neumann) more properly be credited to Cauchy and Frobenius.

1A.7. Let G be a finite group, and suppose that $H < G$ is a proper subgroup. Show that the number of elements of G that do not lie in any conjugate of H is at least $|H|$.

Hint. Let χ be the permutation character associated with the right-multiplication action of G on the right cosets of H . Then $\sum \chi(g) = |G|$, where the sum runs over $g \in G$. Show that $\sum \chi(h) \geq 2|H|$, where here, the sum runs over $h \in H$. Use this information to get an estimate on the number of elements of G where χ vanishes.

1A.8. Let G be a finite group, let $n > 0$ be an integer, and let C be the additive group of the integers modulo n . Let Ω be the set of n -tuples (x_1, x_2, \dots, x_n) of elements of G such that $x_1 x_2 \cdots x_n = 1$.

(a) Show that C acts on Ω according to the formula

$$(x_1, x_2, \dots, x_n) \cdot k = (x_{1+k}, x_{2+k}, \dots, x_{n+k}),$$

where $k \in C$ and the subscripts are interpreted modulo n .

- (b) Now suppose that $n = p$ is a prime number that divides $|G|$. Show that p divides the number of C -orbits of size 1 on Ω , and deduce that the number of elements of order p in G is congruent to $-1 \pmod p$.

Note. In particular, if a prime p divides $|G|$, then G has at least one element of order p . This is a theorem of Cauchy, and the proof in this problem is due to J. H. McKay. Cauchy's theorem can also be derived as a corollary of Sylow's theorem. Alternatively, a proof of Sylow's theorem different from Wielandt's can be based on Cauchy's theorem. (See Problem 1B.4.)

1A.9. Suppose $|G| = pm$, where $p > m$ and p is prime. Show that G has a unique subgroup of order p .

1A.10. Let $H \subseteq G$.

- (a) Show that $|\mathbf{N}_G(H) : H|$ is equal to the number of right cosets of H in G that are invariant under right multiplication by H .
- (b) Suppose that $|H|$ is a power of the prime p and that $|G : H|$ is divisible by p . Show that $|\mathbf{N}_G(H) : H|$ is divisible by p .

1B

Fix a prime number p . A finite group whose order is a power of p is called a **p -group**. It is often convenient, however, to use this nomenclature somewhat carelessly, and to refer to a group as a “ p -group” even if there is no particular prime p under consideration. For example, in proving some theorem, one might say: it suffices to check that the result holds for p -groups. What is meant here, of course, is that it suffices to show that the theorem holds for all p -groups for all primes p .

We mention that, although in this book a p -group is required to be finite, it is also possible to define infinite p -groups. The more general definition is that a (not necessarily finite) group G is a p -group if every element of G has finite p -power order. Of course, if G is finite, then by Lagrange's theorem, every element of G has order dividing $|G|$, and so if $|G|$ is a power of p , it follows that the order of every element is a power of p , and hence G is a p -group according to the more general definition. Conversely, if G is finite and has the property that the order of every element is a power of p , then clearly, G can have no element of order q for any prime q different from p . It follows by Cauchy's theorem (Problem 1A.8) that no prime $q \neq p$ can divide $|G|$, and thus $|G|$ must be a power of p , and this shows that the two definitions of “ p -group” are equivalent for finite groups.

Again, fix a prime p . A subgroup S of a finite group G is said to be a **Sylow p -subgroup** of G if $|S|$ is a power of p and the index $|G : S|$ is

not divisible by p . An alternative formulation of this definition relies on the observation that every positive integer can be (uniquely) factored as a power of the given prime p times some integer not divisible by p . In particular, if we write $|G| = p^a m$, where $a \geq 0$ and p does not divide $m \geq 1$, then a subgroup S of G is a Sylow p -subgroup of G precisely when $|S| = p^a$. In other words, a Sylow p -subgroup of G is a p -subgroup S whose order is as large as is permitted by Lagrange's theorem, which requires that $|S|$ must divide $|G|$. We mention two trivial cases: if $|G|$ is not divisible by p , then the identity subgroup is a Sylow p -subgroup of G , and if G is a p -group, then G is a Sylow p -subgroup of itself. The Sylow existence theorem asserts that Sylow subgroups *always* exist.

1.7. Theorem (Sylow E). *Let G be a finite group, and let p be a prime. Then G has a Sylow p -subgroup.*

The Sylow E-theorem can be viewed as a partial converse of Lagrange's theorem. Lagrange asserts that if H is a subgroup of G and $|H| = k$, then k divides $|G|$. The converse, which in general is false, would say that if k is a positive integer that divides $|G|$, then G has a subgroup of order k . (The smallest example of the failure of this assertion is to take G to be the alternating group A_4 of order 12; this group has no subgroup of order 6.) But if k is a power of a prime, we shall see that G actually does have a subgroup of order k . If k is the largest power of p that divides $|G|$, the desired subgroup of order k is a Sylow p -subgroup; for smaller powers of p , we will prove that a Sylow p -subgroup of G necessarily has a subgroup of order k .

We are ready now to begin work toward the proof of the Sylow E-theorem. We start with a purely arithmetic fact about binomial coefficients.

1.8. Lemma. *Let p be a prime number, and let $a \geq 0$ and $m \geq 1$ be integers. Then*

$$\binom{p^a m}{p^a} \equiv m \pmod{p}.$$

Proof. Consider the polynomial $(1 + X)^p$. Since p is prime, it is easy to see that the binomial coefficients $\binom{p}{i}$ are divisible by p for $1 \leq i \leq p - 1$, and thus we can write $(1 + X)^p \equiv 1 + X^p \pmod{p}$. (The assertion that these polynomials are congruent modulo p means that the coefficients of corresponding powers of X are congruent modulo p .) Applying this fact a second time, we see that $(1 + X)^{p^2} \equiv (1 + X^p)^p \equiv 1 + X^{p^2} \pmod{p}$. Continuing like this, we deduce that $(1 + X)^{p^a} \equiv 1 + X^{p^a} \pmod{p}$, and thus

$$(1 + X)^{p^a m} \equiv (1 + X^{p^a})^m \pmod{p}.$$

Since these polynomials are congruent, the coefficients of corresponding terms are congruent modulo p , and the result follows by considering the coefficient of X^{p^a} on each side. ■

Proof of the Sylow E-theorem (Wielandt). Write $|G| = p^a m$, where $a \geq 0$ and p does not divide m . Let Ω be the set of all subsets of G having cardinality p^a , and observe that G acts by right multiplication on Ω . Because of this action, Ω is partitioned into orbits, and consequently, $|\Omega|$ is the sum of the orbit sizes. But

$$|\Omega| = \binom{p^a m}{p^a} \equiv m \not\equiv 0 \pmod{p},$$

and so $|\Omega|$ is not divisible by p , and it follows that there is some orbit \mathcal{O} such that $|\mathcal{O}|$ is not divisible by p .

Now let $X \in \mathcal{O}$, and let $H = G_X$ be the stabilizer of X in G . By the fundamental counting principle, $|\mathcal{O}| = |G|/|H|$, and since p does not divide $|\mathcal{O}|$ and p^a divides $|G|$, we conclude that p^a must divide $|H|$, and in particular $p^a \leq |H|$.

Since H stabilizes X under right multiplication, we see that if $x \in X$, then $xH \subseteq X$, and thus $|H| = |xH| \leq |X| = p^a$, where the final equality holds since $X \in \Omega$. We now have $|H| = p^a$, and since H is a subgroup, it is a Sylow subgroup of G , as wanted. ■

In Problem 1A.8, we sketched a proof of Cauchy's theorem. We can now give another proof, using the Sylow E-theorem.

1.9. Corollary (Cauchy). *Let G be a finite group, and suppose that p is a prime divisor of $|G|$. Then G has an element of order p .*

Proof. Let S be a Sylow p -subgroup of G , and note that since $|S|$ is the maximum power of p that divides $|G|$, we have $|S| > 1$. Choose a non-identity element x of S , and observe that the order $o(x)$ divides $|S|$ by Lagrange's theorem, and thus $1 < o(x)$ is a power of p . In particular, we can write $o(x) = pm$ for some integer $m \geq 1$, and we see that $o(x^m) = p$, as wanted. ■

We introduce the notation $\text{Syl}_p(G)$ to denote the set of all Sylow p -subgroups of G . The assertion of the Sylow E-theorem, therefore, is that the set $\text{Syl}_p(G)$ is nonempty for all finite groups G and all primes p . The intersection $\bigcap \text{Syl}_p(G)$ of all Sylow p -subgroups of a group G is denoted $\mathbf{O}_p(G)$, and as we shall see, this is a subgroup that plays an important role in finite group theory.

Perhaps this is a good place to digress to review some basic facts about characteristic subgroups. (Some of this material also appears in the appendix.) First, we recall the definition: a subgroup $K \subseteq G$ is **characteristic** in G if every automorphism of G maps K onto itself.

It is often difficult to find all automorphisms of a given group, and so the definition of “characteristic” can be hard to apply directly, but nevertheless, in many cases, it is easy to establish that certain subgroups are characteristic. For example, the center $\mathbf{Z}(G)$, the derived (or commutator) subgroup G' , and the intersection of all Sylow p -subgroups $\mathbf{O}_p(G)$ are characteristic in G . More generally, any subgroup that can be described unambiguously as “*the* something” is characteristic. It is essential that the description using the definite article be unambiguous, however. Given a subgroup $H \subseteq G$, for example, we cannot conclude that the normalizer $\mathbf{N}_G(H)$ or the center $\mathbf{Z}(H)$ is characteristic in G . Although these subgroups are described using “the”, the descriptions are not unambiguous because they depend on the choice of H . We can say, however, that $\mathbf{Z}(G')$ is characteristic in G because it is *the* center of *the* derived subgroup; it does not depend on any unspecified subgroups.

A good way to see why “the something” subgroups must be characteristic is to imagine two groups G_1 and G_2 , with an isomorphism $\theta : G_1 \rightarrow G_2$. Since isomorphisms preserve “group theoretic” properties, it should be clear that θ maps the center $\mathbf{Z}(G_1)$ onto $\mathbf{Z}(G_2)$, and indeed θ maps each unambiguously defined subgroup of G_1 onto the corresponding subgroup of G_2 . Now specialize to the case where G_1 and G_2 happen to be the same group G , so θ is an automorphism of G . Since in the general case, we know that $\theta(\mathbf{Z}(G_1)) = \mathbf{Z}(G_2)$, we see that when $G_1 = G = G_2$, we have $\theta(\mathbf{Z}(G)) = \mathbf{Z}(G)$, and similarly, if we consider any “the something” subgroup in place of the center.

Of course, characteristic subgroups are automatically normal. This is because the definition of normality requires only that the subgroup be mapped onto itself by *inner* automorphisms while characteristic subgroups are mapped onto themselves by all automorphisms. We have seen that some characteristic subgroups are easily recognized, and it follows that these subgroups are obviously and automatically normal. For example, the subgroup $\mathbf{O}_p(G)$ is normal in G for all primes p .

The fact that characteristic subgroups are normal remains true in an even more general context. The following, which we presume is already known to most readers of this book, is extremely useful. (This result also appears in the appendix.)

1.10. Lemma. *Let $K \subseteq N \subseteq G$, where G is a group, N is a normal subgroup of G and K is a characteristic subgroup of N . Then $K \triangleleft G$.*

Proof. Let $g \in G$. Then conjugation by g maps N onto itself, and it follows that the restriction of this conjugation map to N is an automorphism of N . (But note that it is not necessarily an inner automorphism of N .) Since K is characteristic in N , it is mapped onto itself by this automorphism of N , and thus $K^g = K$, and it follows that $K \triangleleft G$. ■

Problems 1B

1B.1. Let $S \in \text{Syl}_p(G)$, where G is a finite group.

- (a) Let $P \subseteq G$ be a p -subgroup. Show that PS is a subgroup if and only if $P \subseteq S$.
- (b) If $S \triangleleft G$, show that $\text{Syl}_p(G) = \{S\}$, and deduce that S is characteristic in G .

Note. Of course, it would be “cheating” to do problems in this section using theory that we have not yet developed. In particular, you should avoid using the Sylow C-theorem, which asserts that every two Sylow p -subgroups of G are conjugate in G .

1B.2. Show that $\mathbf{O}_p(G)$ is the unique largest normal p -subgroup of G . (This means that it is a normal p -subgroup of G that contains every other normal p -subgroup of G .)

1B.3. Let $S \in \text{Syl}_p(G)$, and write $N = \mathbf{N}_G(S)$. Show that $N = \mathbf{N}_G(N)$.

1B.4. Let $P \subseteq G$ be a p -subgroup such that $|G : P|$ is divisible by p . Using Cauchy’s theorem, but without appealing to Sylow’s theorem, show that there exists a subgroup Q of G containing P , and such that $|Q : P| = p$. Deduce that a maximal p -subgroup of G (which obviously must exist) must be a Sylow p -subgroup of G .

Hint. Use Problem 1A.10 and consider the group $\mathbf{N}_G(P)/P$.

Note. Once we know Cauchy’s theorem, this problem yields an alternative proof of the Sylow E-theorem. Of course, to avoid circularity, we appeal to Problem 1A.8 for Cauchy’s theorem, and not to Corollary 1.9.

1B.5. Let π be any set of prime numbers. We say that a finite group H is a π -**group** if every prime divisor of $|H|$ lies in π . Also, a π -subgroup $H \subseteq G$ is a **Hall** π -subgroup of G if no prime dividing the index $|G : H|$ lies in π . (So if $\pi = \{p\}$, a Hall π -subgroup is exactly a Sylow p -subgroup.)

Now let $\theta : G \rightarrow K$ be a surjective homomorphism of finite groups.

- (a) If H is a Hall π -subgroup of G , prove that $\theta(H)$ is a Hall π -subgroup of K .

- (b) Show that every Sylow p -subgroup of K has the form $\theta(H)$, where H is some Sylow p -subgroup of G .
- (c) Show that $|\text{Syl}_p(G)| \geq |\text{Syl}_p(K)|$ for every prime p .

Note. If the set π contains more than one prime number, then a Hall π -subgroup can fail to exist. But a theorem of P. Hall, after whom these subgroups are named, asserts that in the case where G is solvable, Hall π -subgroups always do exist. (See Chapter 3, Section C.) We mention also that Part (b) of this problem would not remain true if “Sylow p -subgroup” were replaced by “Hall π -subgroup”.

1B.6. Let G be a finite group, and let $K \subseteq G$ be a subgroup. Suppose that $H \subseteq G$ is a Hall π -subgroup, where π is some set of primes. Show that if HK is a subgroup, then $H \cap K$ is a Hall π -subgroup of K .

Note. In particular, K has a Hall π -subgroup if either H or K is normal in G since in that case, HK is guaranteed to be a subgroup.

1B.7. Let G be a finite group, and let π be any set of primes.

- (a) Show that G has a (necessarily unique) normal π -subgroup N such that $N \supseteq M$ whenever $M \triangleleft G$ is a π -subgroup.
- (b) Show that the subgroup N of Part (a) is contained in every Hall π -subgroup of G .
- (c) Assuming that G has a Hall π -subgroup, show that N is exactly the intersection of all of the Hall π -subgroups of G .

Note. The subgroup N of this problem is denoted $\mathbf{O}_\pi(G)$. Because of the uniqueness in (b), it follows that this subgroup is characteristic in G . Finally, we note that if p is a prime number, then, of course, $\mathbf{O}_{\{p\}}(G) = \mathbf{O}_p(G)$.

1B.8. Let G be a finite group, and let π be any set of primes.

- (a) Show that G has a (necessarily unique) normal subgroup N such that G/N is a π -group and $M \supseteq N$ whenever $M \triangleleft G$ and G/M is a π -group.
- (b) Show that the subgroup N of Part (a) is generated by the set of all elements of G that have order not divisible by any prime in π .

Note. The characteristic subgroup N of this problem is denoted $\mathbf{O}^\pi(G)$. Also, we recall that the subgroup generated by a subset of G is the (unique) smallest subgroup that contains that set.

1C

We are now ready to study in greater detail the nonempty set $\text{Syl}_p(G)$ of Sylow p -subgroups of a finite group G .

1.11. Theorem. *Let P be an arbitrary p -subgroup of a finite group G , and suppose that $S \in \text{Syl}_p(G)$. Then $P \subseteq S^g$ for some element $g \in G$.*

Proof. Let $\Omega = \{Sx \mid x \in G\}$, the set of right cosets of S in G , and note that $|\Omega| = |G : S|$ is not divisible by p since S is a Sylow p -subgroup of G . We know that G acts by right multiplication on Ω , and thus P acts too, and Ω is partitioned into P -orbits. Also, since $|\Omega|$ is not divisible by p , there must exist some P -orbit \mathcal{O} such that $|\mathcal{O}|$ is not divisible by p .

By the fundamental counting principle, $|\mathcal{O}|$ is the index in P of some subgroup. It follows that $|\mathcal{O}|$ divides $|P|$, which is a power of p . Then $|\mathcal{O}|$ is both a power of p and not divisible by p , and so the only possibility is that $|\mathcal{O}| = 1$. Recalling that all members of Ω are right cosets of S in G , we can suppose that the unique member of \mathcal{O} is the coset Sg .

Since Sg is alone in a P -orbit, it follows that it is fixed under the action of P , and thus $Sgu = Sg$ for all elements $u \in P$. Then $gu \in Sg$, and hence $u \in g^{-1}Sg = S^g$. Thus $P \subseteq S^g$, as required. ■

If S is a Sylow p -subgroup of G , and $g \in G$ is arbitrary, then the conjugate S^g is a subgroup having the same order as S . Since the only requirement on a subgroup that is needed to qualify it for membership in the set $\text{Syl}_p(G)$ is that it have the correct order, and since $S \in \text{Syl}_p(G)$ and $|S^g| = |S|$, it follows that S^g also lies in $\text{Syl}_p(G)$. In fact *every* member of $\text{Syl}_p(G)$ arises this way: as a conjugate of S . This is the essential content of the Sylow conjugacy theorem. Putting it another way: the conjugation action of G on $\text{Syl}_p(G)$ is transitive.

1.12. Theorem (Sylow C). *If S and T Sylow p -subgroups of a finite group G , then $T = S^g$ for some element $g \in G$.*

Proof. Applying Theorem 1.11 with T in place of P , we conclude that $T \subseteq S^g$ for some element $g \in G$. But since both S and T are Sylow p -subgroups, we have $|T| = |S| = |S^g|$, and so the containment of the previous sentence must actually be an equality. ■

The Sylow C-theorem yields an alternative proof of Problem IB.1(b), which asserts that if a group G has a normal Sylow p -subgroup S , then S is the only Sylow p -subgroup of G . Indeed, by the Sylow C-theorem, if $T \in \text{Syl}_p(G)$, then we can write $T = S^g = S$, where the second equality is a consequence of the normality of S .

A frequently used application of the Sylow C-theorem is the so-called “Frattini argument”, which we are about to present. Perhaps the reason that this result is generally referred to as an “argument” rather than as a “lemma” or “theorem” is that variations on its proof are used nearly as often as its statement.

1.13. Lemma (Frattini Argument). *Let $N \triangleleft G$ where N is finite, and suppose that $P \in \text{Syl}_p(N)$. Then $G = \mathbf{N}_G(P)N$.*

Proof. Let $g \in G$, and note that $P^g \subseteq N^g = N$, and thus P^g is a subgroup of N having the same order as the Sylow p -subgroup P . It follows that $P^g \in \text{Syl}_p(N)$, and so by the Sylow C-theorem applied in N , we deduce that $(P^g)^n = P$, for some element $n \in N$. Since $P^{gn} = P$, we have $gn \in \mathbf{N}_G(P)$, and so $g \in \mathbf{N}_G(P)n^{-1} \subseteq \mathbf{N}_G(P)N$. But $g \in G$ was arbitrary, and we deduce that $G = \mathbf{N}_G(P)N$, as required. ■

By definition, a Sylow p -subgroup of a finite group G is a p -subgroup that has the largest possible order consistent with Lagrange’s theorem. By the Sylow E-theorem, we can make a stronger statement: a subgroup whose order is maximal among the orders of all p -subgroups of G is a Sylow p -subgroup. An even stronger assertion of this type is that every maximal p -subgroup of G is a Sylow p -subgroup. Here, “maximal” is to be interpreted in the sense of containment: a subgroup H of G is maximal with some property if there is no subgroup $K > H$ that has the property. The truth of this assertion is the essential content of the Sylow “development” theorem.

1.14. Theorem (Sylow D). *Let P be a p -subgroup of a finite group G . Then P is contained in some Sylow p -subgroup of G .*

Proof. Let $S \in \text{Syl}_p(G)$. Then by Theorem 1.11, we know that $P \subseteq S^g$ for some element $g \in G$. Also, since $|S^g| = |S|$, we know that S^g is a Sylow p -subgroup of G . ■

Given a finite group G , we consider next the question of how many Sylow p -subgroups G has. To facilitate this discussion, we introduce the (not quite standard) notation $n_p(G) = |\text{Syl}_p(G)|$. (Occasionally, when the group we are considering is clear from the context, we will simply write n_p instead of $n_p(G)$.)

First, by the Sylow C-theorem, we know that $\text{Syl}_p(G)$ is a single orbit under the conjugation action of G . The following is then an immediate consequence.

1.15. Corollary. *Let $S \in \text{Syl}_p(G)$, where G is a finite group. Then $n_p(G) = |G : \mathbf{N}_G(S)|$.*

Proof. Since $n_p(G) = |\text{Syl}_p(G)|$ is the total number of conjugates of S in G , the result follows by Corollary 1.6. ■

In particular, it follows that $n_p(G)$ divides $|G|$, but we can say a bit more. If $S \in \text{Syl}_p(G)$, then of course, $S \subseteq \mathbf{N}_G(S)$ since S is a subgroup, and thus $|G : S| = |G : \mathbf{N}_G(S)| |\mathbf{N}_G(S) : S|$. Also, $n_p(G) = |G : \mathbf{N}_G(S)|$, and hence $n_p(G)$ divides $|G : S|$. In other words, if we write $|G| = p^a m$, where p does not divide m , we see that $n_p(G)$ divides m . (We mention that the integer m is often referred to as the p' -part of $|G|$.)

The information that $n_p(G)$ divides the p' -part of $|G|$ becomes even more useful when it is combined with the fact (probably known to most readers) that $n_p(G) \equiv 1 \pmod{p}$ for all groups G . In fact, there is a useful stronger congruence constraint, which may not be quite so well known. Before we present our theorem, we mention that if $S, T \in \text{Syl}_p(G)$, then $|S| = |T|$, and thus $|S : S \cap T| = |S|/|S \cap T| = |T|/|S \cap T| = |T : S \cap T|$. The statement of the following result, therefore, is not really as asymmetric as it may appear.

1.16. Theorem. *Suppose that G is a finite group such that $n_p(G) > 1$, and choose distinct Sylow p -subgroups S and T of G such that the order $|S \cap T|$ is as large as possible. Then $n_p(G) \equiv 1 \pmod{|S : S \cap T|}$.*

1.17. Corollary. *If G is a finite group and p is a prime, then $n_p(G) \equiv 1 \pmod{p}$.*

Proof. If $n_p(G) = 1$, there is nothing to prove. Otherwise, Theorem 1.16 applies, and there exist distinct members $S, T \in \text{Syl}_p(G)$ such that $n_p(G) \equiv 1 \pmod{|S : S \cap T|}$, and thus it suffices to show that $|S : S \cap T|$ is divisible by p . But $|S : S \cap T| = |T : S \cap T|$ is certainly a power of p , and it exceeds 1 since otherwise $S = S \cap T = T$, which is not the case because S and T are distinct. ■

In order to see how Theorem 1.16 can be used, consider a group G of order $21,952 = 2^6 \cdot 7^3$. We know that n_7 must divide $2^6 = 64$, and it must be congruent to 1 modulo 7. We see, therefore, that n_7 must be one of 1, 8 or 64. Suppose that G does not have a normal Sylow 7-subgroup, so that $n_7 > 1$. Since neither 8 nor 64 is congruent to 1 modulo $7^2 = 49$, we see by Theorem 1.16 that there exist distinct Sylow 7-subgroups S and T of G such that $|S : S \cap T| = 7$.

Let's pursue this a bit further. Write $D = S \cap T$ in the above situation, and note that since $|S : D| = 7$ is the smallest prime divisor of $|S| = 7^3$, it follows by Problem 1A.1, that $D \triangleleft S$. Similar reasoning shows that also $D \triangleleft T$, and hence S and T are both contained in $N = \mathbf{N}_G(D)$. Now S and T are distinct Sylow 7-subgroups of N , and it follows that $n_7(N) > 1$, and hence $n_7(N) \geq 8$ by Corollary 1.17. Since $n_7(N)$ is a power of 2 that

divides $|N|$, we deduce that 2^3 divides $|N|$. Since also 7^3 divides $|N|$, we have $|G : N| \leq 8$.

We can use what we have established to show that a group G of order 21,952 cannot be simple. Indeed, if $n_7(G) = 1$, then G has a normal subgroup of order 7^3 , and so is not simple. Otherwise, our subgroup N has index at most 8, and we see that $|G|$ does not divide $|G : N|!$. By the $n!$ -theorem (Corollary 1.3), therefore, G cannot be simple if $N < G$. Finally, if $N = G$ then $D < G$ and G is not simple in this case too.

In the last case, where $D < G$, we see that D is contained in all Sylow 7-subgroups of G , and thus D is the intersection of *every* two distinct Sylow 7-subgroups of G . In most situations, however, Theorem 1.16 can be used to prove only the existence of some pair of distinct Sylow subgroups with a “large” intersection; it does not usually follow that every such pair has a large intersection.

To prove Theorem 1.16, we need the following.

1.18. Lemma. *Let $P \in \text{Syl}_p(G)$, where G is a finite group, and suppose that Q is a p -subgroup of $\mathbf{N}_G(P)$. Then $Q \subseteq P$.*

Proof. We apply Sylow theory in the group $N = \mathbf{N}_G(P)$. Clearly, P is a Sylow p -subgroup of N , and since $P < N$, we deduce that P is the only Sylow p -subgroup of N . By the Sylow D-theorem, however, the p -subgroup Q of N must be contained in some Sylow p -subgroup. The only possibility is $Q \subseteq P$, as required. ■

An alternative method of proof for Lemma 1.18 is to observe that since $Q \subseteq \mathbf{N}_G(P)$, it follows that $QP = PQ$. Then QP is a subgroup, and it is easy to see that it is a p -subgroup that contains the Sylow p -subgroup P . It follows that $P = QP \supseteq Q$, as wanted.

Proof of Theorem 1.16. Let S act on the set $\text{Syl}_p(G)$ by conjugation. One orbit is the set $\{S\}$, of size 1, and so if we can show that all other orbits have size divisible by $|S : S \cap T|$, it will follow that $n_p(G) = |\text{Syl}_p(G)| \equiv 1 \pmod{|S : S \cap T|}$, as wanted. Let \mathcal{O} be an arbitrary S -orbit in $\text{Syl}_p(G)$ other than $\{S\}$ and let $P \in \mathcal{O}$, so that $P \neq S$. By the fundamental counting principle, $|\mathcal{O}| = |S : Q|$, where Q is the stabilizer of P in S under conjugation. Then $Q \subseteq \mathbf{N}_G(P)$, and so $Q \subseteq P$ by Lemma 1.18. But also $Q \subseteq S$, and thus $|Q| \leq |S \cap P| \leq |S \cap T|$; where the latter inequality is a consequence of the fact that $|S \cap T|$ is as large as possible among intersections of two distinct Sylow p -subgroups of G . It follows that $|\mathcal{O}| = |S : Q| \geq |S : S \cap T|$. But since the integers $|\mathcal{O}|$ and $|S : S \cap T|$ are powers of p and $|\mathcal{O}| \geq |S : S \cap T|$, we conclude that $|\mathcal{O}|$ is a multiple of $|S : S \cap T|$. This completes the proof. ■

Problems 1C

1C.1. Let $P \in \text{Syl}_p(G)$, and suppose that $\mathbf{N}_G(P) \subseteq H \subseteq G$, where H is a subgroup. Prove that $H = \mathbf{N}_G(H)$.

Note. This generalizes Problem 1B.3.

1C.2. Let $H \subseteq G$, where G is a finite group.

- (a) If $P \in \text{Syl}_p(H)$, prove that $P = H \cap S$ for some member $S \in \text{Syl}_p(G)$.
- (b) Show that $n_p(H) \leq n_p(G)$ for all primes p .

1C.3. Let G be a finite group, and let X be the subset of G consisting of all elements whose order is a power of p , where p is some fixed prime.

- (a) Show that $X = \bigcup \text{Syl}_p(G)$.
- (b) Show that if p divides $|G|$, then $|X|$ is divisible by p .

Hint. For (b), let a Sylow p -subgroup act on X .

1C.4. Let $|G| = 120 = 2^3 \cdot 3 \cdot 5$. Show that G has a subgroup of index 3 or a subgroup of index 5 (or both).

Hint. Analyze separately the four possibilities for $n_2(G)$.

1C.5. Let $P \in \text{Syl}_p(G)$, where $G = A_{p+1}$, the alternating group on $p+1$ symbols. Show that $|\mathbf{N}_G(P)| = p(p-1)/2$.

Hint. Count the elements of order p in G .

1C.6. Let $G = HK$, where H and K are subgroups, and fix a prime p .

- (a) Show that there exists $P \in \text{Syl}_p(G)$ such that $P \cap H \in \text{Syl}_p(H)$ and $P \cap K \in \text{Syl}_p(K)$.
- (b) If P is as in (a), show that $P = (P \cap H)(P \cap K)$.

Hint. For (a), first choose $Q \in \text{Syl}_p(G)$ and $g \in G$ such that $Q \cap H \in \text{Syl}_p(H)$ and $Q^g \cap K \in \text{Syl}_p(K)$. Write $g = hk$, with $h \in H$ and $k \in K$.

1C.7. Let G be a finite group in which every maximal subgroup has prime index, and let p be the largest prime divisor of $|G|$. Show that a Sylow p -subgroup of G is normal.

Hint. Otherwise, let M be a maximal subgroup of G containing $\mathbf{N}_G(P)$, where $P \in \text{Syl}_p(G)$. Compare $n_p(M)$ and $n_p(G)$.

1C.8. Let P be a Sylow p -subgroup of G . Show that for every nonnegative integer a , the numbers of subgroups of order p^a in P and in G are congruent modulo p .

Note. If $p^a = |P|$, then the number of subgroups of order p^a in P is clearly 1, and it follows that the number of such subgroups in G is congruent to 1 modulo p . This provides a somewhat different proof that $n_p(G) \equiv 1 \pmod{p}$. It is true in general that if $p^a \leq |P|$, then the number of subgroups of order p^a in P is congruent to 1 modulo p , and thus it follows that if p^a divides the order of an arbitrary finite group G , then the number of subgroups of order p^a in G is congruent to 1 mod p .

1D

We now digress from our study of Sylow theory in order to review some basic facts about p -groups and nilpotent groups. Also, we discuss the Fitting subgroup, and in the problems at the end of the section, we present some results about the Frattini subgroup.

Although p -groups are not at all typical of finite groups in general, they play a prominent role in group theory, and they are ubiquitous in the study of finite groups. This ubiquity is, of course, a consequence of the Sylow theorems, and perhaps that justifies our digression.

We should mention that although their structure is atypical when compared with finite groups in general, p -groups are, nevertheless, extremely abundant in comparison with non- p -groups. There are, for example, 2,328 isomorphism types of groups of order $128 = 2^7$; the number of types of order $256 = 2^8$ is 56,092; for $512 = 2^9$ the number is 10,494,213; and there are exactly 49,487,365,422 isomorphism types of groups of order $1,024 = 2^{10}$. (These numbers were computed by a remarkable algorithm for counting p -groups that was developed by E. O'Brien.)

There is an extensive theory of finite p -groups (and also of their infinite cousins, pro- p -groups), and there are several books entirely devoted to them. Our brief presentation here will be quite superficial; later, we study p -groups a bit more deeply, but still, we shall see only a tiny part of what is known.

Perhaps the most fundamental fact about p -groups is that nontrivial finite p -groups have nontrivial centers. (By our definition, “ p -group” means “finite p -group”, but we included the redundant adjective in the previous sentence and in what follows in order to stress the fact that finiteness is essential here. Infinite p -groups can have trivial centers, and in fact, they can be simple groups.)

In fact, a stronger statement is true.

1.19. Theorem. *Let P be a finite p -group and let N be a nonidentity normal subgroup of P . Then $N \cap \mathbf{Z}(P) > 1$. In particular, if P is nontrivial, then $\mathbf{Z}(P) > 1$.*

Proof. Since $N \triangleleft P$, we can let P act on N by conjugation, and we observe that $N \cap \mathbf{Z}(P)$ is exactly the set of elements of N that lie in orbits of size 1. By the fundamental counting principle, every orbit has p -power size, and so each nontrivial orbit (*i.e.*, orbit of size exceeding 1) has size divisible by p . Since the set $N - (N \cap \mathbf{Z}(P))$ is a union of such orbits, we see that $|N| - |N \cap \mathbf{Z}(P)|$ is divisible by p , and thus $|N \cap \mathbf{Z}(P)| \equiv |N| \equiv 0 \pmod{p}$, where the second congruence follows because N is a nontrivial subgroup. Now $N \cap \mathbf{Z}(P)$ contains the identity element, and so $|N \cap \mathbf{Z}(P)| > 0$. It follows that $|N \cap \mathbf{Z}(P)| \geq p > 1$, and hence $N \cap \mathbf{Z}(P)$ is nontrivial, as required. The final assertion follows by taking $N = P$. ■

It is now easy to show that (finite, of course) p -groups are nilpotent, and thus we can obtain additional information about p -groups by studying general nilpotent groups. But first, we review some definitions.

A finite collection of normal subgroups N_i of a (not necessarily finite) group G is a **normal series** for G provided that

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = G.$$

This normal series is a **central series** if in addition, we have $N_i/N_{i-1} \subseteq \mathbf{Z}(G/N_{i-1})$ for $1 \leq i \leq r$. Finally, a group G is **nilpotent** if it has a central series. It is worth noting that subgroups and factor groups of nilpotent groups are themselves nilpotent, although we omit the easy proofs of these facts.

Given any group G , we can attempt to construct a central series as follows. (But of course, this attempt is doomed to failure unless G is nilpotent.) We start by defining $Z_0 = 1$ and $Z_1 = \mathbf{Z}(G)$. The **second center** Z_2 is defined to be the unique subgroup such that $Z_2/Z_1 = \mathbf{Z}(G/Z_1)$. (Note that Z_2 exists and is normal in G by the correspondence theorem.) We continue like this, inductively defining Z_n for $n > 0$ so that $Z_n/Z_{n-1} = \mathbf{Z}(G/Z_{n-1})$. The chain of normal subgroups

$$1 = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots$$

constructed this way is called the **upper central series** of G . We hasten to point out, however, that in general, the upper central series may not actually be a central series for G because it may happen that $Z_i < G$ for all i . In other words, the upper central series may never reach the whole group G . But if $Z_r = G$ for some integer r , then $\{Z_i \mid 0 \leq i \leq r\}$ is a true central series, and G is nilpotent.

Conversely, if G is nilpotent, the upper central series of G really is a central series. For finite groups G , this is especially easy to prove.

1.20. Lemma. *Let G be finite. Then the following are equivalent.*

- (1) G is nilpotent.
- (2) Every nontrivial homomorphic image of G has a nontrivial center.
- (3) G appears as a member of its upper central series.

Proof. We have already remarked that homomorphic images of nilpotent groups are nilpotent. Also, since the first nontrivial term of a central series for a nilpotent group is contained in the center of the group, it follows that nontrivial nilpotent groups have nontrivial centers. This shows that (1) implies (2).

Assuming (2) now, it follows that if $Z_i < G$, where Z_i is a term in the upper central series for G , then $Z_{i+1}/Z_i = \mathbf{Z}(G/Z_i)$ is nontrivial, and thus $Z_i < Z_{i+1}$. Since G is finite and the proper terms of the upper central series are strictly increasing, we see that not every term can be proper, and this establishes (3).

Finally, (3) guarantees that the upper central series for G is actually a central series, and thus G is nilpotent, proving (1). ■

If P is a finite p -group, then of course, every homomorphic image of P is also a finite p -group, and thus every nontrivial homomorphic image of P has a nontrivial center. It follows by Lemma 1.20, therefore, that finite p -groups are nilpotent. In fact, we shall see in Theorem 1.26 that much more is true: a finite group G is nilpotent if and only if every Sylow subgroup of G is normal.

Next, we show that the terms of the upper central series of a nilpotent group contain the corresponding terms of an arbitrary central series, and this explains why the upper central series is called “upper”. It also provides an alternative proof of the implication (1) \Rightarrow (3) of Lemma 1.20, without the assumption that G is finite.

1.21. Theorem. *Let G be a (not necessarily finite) nilpotent group with central series*

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = G,$$

and as usual, let

$$1 = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots$$

be the upper central series for G . Then $N_i \subseteq Z_i$ for $0 \leq i \leq r$, and in particular, $Z_r = G$.

Proof. We prove that $N_i \subseteq Z_i$ by induction on i . Since $Z_0 = 1 = N_0$, we can suppose that $i > 0$, and by the inductive hypothesis, we can assume that $N_{i-1} \subseteq Z_{i-1}$. For notational simplicity, write $N = N_{i-1}$ and $Z = Z_{i-1}$, and observe that since $N \subseteq Z$, there is a natural surjective homomorphism $\theta : G/N \rightarrow G/Z$, defined by $\theta(Ng) = Zg$ for elements $g \in G$. (This map is well defined since Zg is the unique coset of Z that contains Ng , and so $\theta(Ng)$ depends only on the coset Ng and not on the element g .)

Since θ is surjective, it carries central elements of G/N to central elements of G/Z , and since N_i/N is central in G/N , it is mapped by θ into $\mathbf{Z}(G/Z) = Z_i/Z$. If $x \in N_i$, therefore, it follows that $Zx = \theta(Nx) \in Z_i/Z$, and thus $x \in Z_i$, as required. ■

If G is an arbitrary nilpotent group, then G is a term of its upper central series, which, therefore is a true central series. We have $G = Z_r$ for some integer $r \geq 0$, and the smallest integer r for which this happens is called the **nilpotence class** of G . Thus nontrivial abelian groups have nilpotence class 1, and the groups of nilpotence class 2 are exactly the nonabelian groups G such that $G/\mathbf{Z}(G)$ is abelian.

Since the upper central series of the nilpotent group G is really a central series, we see that if G has nilpotence class r , then it has a central series of length r . (In other words, the series has r containments and $r+1$ terms.) By Theorem 1.21, we see that G cannot have a central series of length smaller than r , and thus the nilpotence class of a nilpotent group is exactly the length of its shortest possible central series. In some sense, the nilpotence class can be viewed as a measure of how far from being abelian a nilpotent group is.

One of the most useful facts about nilpotent groups, and thus also about finite p -groups, is that “normalizers grow”.

1.22. Theorem. *Let $H < G$, where G is a (not necessarily finite) nilpotent group. Then $\mathbf{N}_G(H) > H$.*

Before we proceed with the (not very difficult) proof of Theorem 1.22, we digress to discuss the “bar convention”, which provides a handy notation for dealing with factor groups. Suppose that $N \triangleleft G$, where G is an arbitrary group. We write \overline{G} to denote the factor group G/N , and we think of the overbar as the name of the canonical homomorphism from G onto \overline{G} . If $g \in G$ is any element, therefore, we write \overline{g} to denote the image of g in \overline{G} , and so we see that \overline{g} is simply another name for the coset Ng . Also, if $H \subseteq G$ is any subgroup, then \overline{H} is the image of H in \overline{G} .

By the correspondence theorem, the homomorphism “overbar” defines a bijection from the set of those subgroups of G that contain N onto the set of all subgroups of \overline{G} . Every subgroup of \overline{G} , therefore, has the form \overline{H} for

some subgroup $H \subseteq G$, and although there are usually many subgroups of G whose image in \overline{G} is the given subgroup \overline{H} , exactly one of them contains N . If $H \subseteq G$ is arbitrary, we see that $\overline{HN} = \overline{H}\overline{N} = \overline{H}$ since overbar is a homomorphism and N is its kernel. It follows that HN is the unique subgroup containing N whose image in \overline{G} is \overline{H} . In particular, since indices of corresponding subgroups are equal, we have $|\overline{G} : \overline{H}| = |G : NH|$ for all subgroups $H \subseteq G$.

The correspondence theorem also yields information about normality. If $N \subseteq H \subseteq K \subseteq G$, then $H \triangleleft K$ if and only if $\overline{H} \triangleleft \overline{K}$. In particular, if $N \subseteq H$, then since $H \subseteq \mathbf{N}_G(H)$, we see that $\overline{H} \triangleleft \overline{\mathbf{N}_G(H)}$ and we have $\overline{\mathbf{N}_G(H)} \subseteq \overline{\mathbf{N}_G(\overline{H})}$. In fact, equality holds here. To see this, observe that since $\overline{\mathbf{N}_G(\overline{H})}$ is a subgroup of \overline{G} , it can be written in the form \overline{U} for some (unique) subgroup U with $N \subseteq U \subseteq G$. Then $\overline{H} \triangleleft \overline{U}$, and so $H \triangleleft U$ and $U \subseteq \mathbf{N}_G(H)$. This yields $\overline{\mathbf{N}_G(\overline{H})} = \overline{U} \subseteq \overline{\mathbf{N}_G(H)}$, as claimed.

We will use the bar convention in the following proof.

Proof of Theorem 1.22. Since G is nilpotent, it has (by definition) a central series $\{N_i \mid 0 \leq i \leq r\}$, and we have $N_0 = 1 \subseteq H$ and $N_r = G \not\subseteq H$. It follows that there is some subscript k with $0 \leq k < r$ such that $N_k \subseteq H$ but $N_{k+1} \not\subseteq H$. We will show that in fact, $N_{k+1} \subseteq \mathbf{N}_G(H)$, and it will follow that $\mathbf{N}_G(H) > H$, as required.

Write $\overline{G} = G/N_k$ and use the bar convention. Since the subgroups N_i form a central series, we have

$$\overline{N_{k+1}} \subseteq \mathbf{Z}(\overline{G}) \subseteq \overline{\mathbf{N}_G(\overline{H})} = \overline{\mathbf{N}_G(H)},$$

where the equality holds because $N_k \subseteq H$. Now because $N_k \subseteq \mathbf{N}_G(H)$, we can remove the overbars to obtain $N_{k+1} \subseteq \mathbf{N}_G(H)$. The proof is now complete. ■

We return now to p -groups, with another application of Theorem 1.19.

1.23. Lemma. *Let P be a finite p -group and suppose that $N < M$ are normal subgroups of P . Then there exists a subgroup $L \triangleleft P$ such that $N \subseteq L \subseteq M$ and $|L : N| = p$.*

Proof. Write $\overline{P} = P/N$ and note that \overline{M} is nontrivial and normal in \overline{P} . Now $\mathbf{Z}(\overline{P}) \cap \overline{M}$ is nontrivial by Theorem 1.19, and so this subgroup contains an element of order p . (Choose any nonidentity element and take an appropriate power.) Because our element is central and of order p , it generates a normal subgroup of order p , and we can write \overline{L} to denote this subgroup, where $N \subseteq L$. Now $\overline{L} \subseteq \overline{M}$, and thus $N \subseteq L \subseteq M$, as wanted. Also, as $\overline{L} \triangleleft \overline{P}$, we see that $L \triangleleft P$. Finally, $|L : N| = |\overline{L}| = p$, as required. ■

1.24. Corollary. *Let P be a p -group of order p^a . Then for every integer b with $0 \leq b \leq a$, there is a subgroup $L \triangleleft P$ such that $|L| = p^b$.*

Proof. The assertion is trivial if $b = 0$, and so we can assume that $b > 0$ and we work by induction on b . By the inductive hypothesis, there exists a subgroup $N \triangleleft P$ such that $|N| = p^{b-1}$ and we can apply Theorem 1.22 (with $M = P$) to produce a subgroup $L \triangleleft P$ with $|L : N| = p$. Then $|L| = p^b$ and the proof is complete. ■

Recall now that the Sylow E-theorem can be viewed as a partial converse to Lagrange's theorem. It asserts that for certain divisors k of an integer n , every group of order n has a subgroup of order k . (The divisors to which we refer, of course, are prime powers k such that n/k is not divisible by the relevant prime.)

We can now enlarge the set of divisors for which we know that the converse of Lagrange's theorem holds.

1.25. Corollary. *Let G be a finite group, and suppose that p^b divides $|G|$, where p is prime and $b \geq 0$ is an integer. Then G has a subgroup of order p^b .*

Proof. Let P be a Sylow p -subgroup of G and write $|P| = p^a$. Since p^b divides $|G|$, we see that $b \leq a$, and the result follows by Corollary 1.23. ■

In fact, in the situation of Corollary 1.25, the number of subgroups of G having order p^b is congruent to 1 modulo p . (By Problem 1C.8 and the note following it, it suffices to prove this in the case where G is a p -group, and while this is not especially difficult, we have decided not to present a proof here.) We mention also that it does not seem to be known whether or not there are any integers n other than powers of primes such that every group of order divisible by n has a subgroup of order n .

Sylow theory is also related to the theory of nilpotent groups in another way: a finite group is nilpotent if and only if all of its Sylow subgroups are normal. In fact, we can say more.

1.26. Theorem. *Let G be a finite group. Then the following are equivalent.*

- (1) G is nilpotent.
- (2) $N_G(H) > H$ for every proper subgroup $H < G$.
- (3) Every maximal subgroup of G is normal.
- (4) Every Sylow subgroup of G is normal.
- (5) G is the (internal) direct product of its nontrivial Sylow subgroups.

Note that in statement (3), a “maximal subgroup” is maximal among *proper* subgroups. But in most other situations, the word “maximal” does not imply proper. If a group G happens to be nilpotent, for example, then the whole group is a maximal nilpotent subgroup of G .

To help with the proof that (4) implies (5), we establish the following.

1.27. Lemma. *Let \mathcal{X} be a collection of finite normal subgroups of a group G , and assume that the orders of the members of \mathcal{X} are pairwise coprime. Then the product $H = \prod \mathcal{X}$ of the members of \mathcal{X} is direct. Also, $|H| = \prod_{X \in \mathcal{X}} |X|$.*

Proof. Certainly $|H| \leq \prod |X|$. Also, by Lagrange’s theorem, $|X|$ divides $|H|$, for every member X of \mathcal{X} , and since the orders of the members of \mathcal{X} are pairwise coprime, it follows that $\prod |X|$ divides $|H|$. We conclude that $|H| = \prod |X|$, as wanted.

Now to see that $\prod X$ is direct, it suffices to show that

$$X \cap \prod \{Y \in \mathcal{X} \mid Y \neq X\} = 1$$

for every member $X \in \mathcal{X}$. This follows since by the previous paragraph, the order of $\prod Y$ for $Y \neq X$ is equal to $\prod |Y|$, and this is coprime to $|X|$. ■

Proof of Theorem 1.26. We saw that (1) implies (2) in Theorem 1.22. That (2) implies (3) is clear, since if $M < G$ is a maximal subgroup, then $\mathbf{N}_G(M) > M$, and so we must have $\mathbf{N}_G(M) = G$.

Now assume (3), and let $P \in \text{Syl}_p(G)$ for some prime p . If $\mathbf{N}_G(P)$ is proper in G , it is contained in some maximal subgroup M , and we have $M \triangleleft G$. Since $P \in \text{Syl}_p(M)$, it follows by Lemma 1.13, the Frattini argument, that $G = \mathbf{N}_G(P)M \subseteq M$, and this is a contradiction. Thus $P \triangleleft G$, and this proves (4).

That (4) implies (5) is immediate from Lemma 1.27. Now assume (5). It is clear that (4) holds, and it follows that (4) also holds for every homomorphic image of G . (See Problem 1B.5.) Since we know that (4) implies (5), we see that every homomorphic image of G is a direct product of p -groups for various primes p . The center of a direct product, however, is the direct product of the centers of the factors, and since nontrivial p -groups have nontrivial centers, it follows that every nonidentity homomorphic image of G has a nontrivial center. We conclude by Lemma 1.20 that G is nilpotent, thereby establishing (1). ■

Recall that $\mathbf{O}_p(G)$ is the unique largest normal p -subgroup of G , by which we mean that it contains every normal p -subgroup. We define the **Fitting subgroup** of G , denoted $\mathbf{F}(G)$, to be the product of the subgroups

$\mathbf{O}_p(G)$ as p runs over the prime divisors of G . Of course, $\mathbf{F}(G)$ is characteristic in G , and in particular, it is normal.

1.28. Corollary. *Let G be a finite group. Then $\mathbf{F}(G)$ is a normal nilpotent subgroup of G . It contains every normal nilpotent subgroup of G , and so it is the unique largest such subgroup.*

Proof. By Lemma 1.27, we know that $|\mathbf{F}(G)|$ is the product of the orders of the subgroups $\mathbf{O}_p(G)$ as p runs over the prime divisors of G . Then $\mathbf{O}_p(G) \in \text{Syl}_p(\mathbf{F}(G))$, and thus $\mathbf{F}(G)$ has a normal Sylow subgroup for each prime. It follows by Theorem 1.26 that $\mathbf{F}(G)$ is nilpotent.

Now let $N \triangleleft G$ be nilpotent. If $P \in \text{Syl}_p(N)$, then $P \triangleleft N$ by Theorem 1.26, and thus P is characteristic in N and hence is normal in G . It follows that $P \subseteq \mathbf{O}_p(G) \subseteq \mathbf{F}(G)$. Since N is the product of its Sylow subgroups and each of these is contained in $\mathbf{F}(G)$, it follows that $N \subseteq \mathbf{F}(G)$, and the proof is complete. ■

1.29. Corollary. *Let K and L be nilpotent normal subgroups of a finite group G . Then KL is nilpotent.*

Proof. We have $K \subseteq \mathbf{F}(G)$ and $L \subseteq \mathbf{F}(G)$, and thus $KL \subseteq \mathbf{F}(G)$. Since $\mathbf{F}(G)$ is nilpotent, it follows that KL is nilpotent. ■

Problems 1D

1D.1. Let $P \in \text{Syl}_p(H)$, where $H \subseteq G$, and suppose that $\mathbf{N}_G(P) \subseteq H$. Show that p does not divide $|G : H|$.

Note. In these problems, we are, as usual, dealing with finite groups.

1D.2. Fix a prime p , and suppose that a subgroup $H \subseteq G$ has the property that $\mathbf{C}_G(x) \subseteq H$ for every element $x \in H$ having order p . Show that p cannot divide both $|H|$ and $|G : H|$.

1D.3. Let $H \subseteq G$ have the property that $H \cap H^g = 1$ for all elements $g \in G - H$.

(a) Show that $\mathbf{N}_G(K) \subseteq H$ for all subgroups K with $1 < K \subseteq H$.

(b) Show that H is a Hall subgroup of G . (Recall that this means that $|H|$ and $|G : H|$ are coprime.)

Note. A subgroup $H < G$ that satisfies the hypothesis of this problem is usually referred to as a **Frobenius complement** in G . In Chapter 6, we give a different definition of a “Frobenius complement”, which, in fact, is equivalent to this one. It is easy to see (as we will show) that a Frobenius complement in the sense of Chapter 6 satisfies the hypothesis of this problem.

What is much more difficult is the theorem of Frobenius, which asserts that if H is a Frobenius complement in G in the sense defined here, then it is, in fact, a Frobenius complement in the sense of Chapter 6. Unfortunately, all known proofs of Frobenius' theorem require character theory, and so we cannot present a proof in this book.

1D.4. Let $G = NH$, where $1 < N \triangleleft G$ and $N \cap H = 1$. Show that H is a Frobenius complement in G (as defined above) if and only if $\mathbf{C}_N(h) = 1$ for all nonidentity elements $h \in H$.

Hint. If x and x^n lie in H , where $n \in N$, observe that $x^{-1}x^n \in N$.

1D.5. Let $H < G$, and suppose that $\mathbf{N}_G(P) \subseteq H$ for all p -subgroups $P \subseteq H$, for all primes p . Show that H is a Frobenius complement in G .

Hint. Observe that the hypothesis is satisfied by $H \cap H^g$ for $g \in G$. If this intersection is nontrivial, consider a nontrivial Sylow subgroup Q of $H \cap H^g$ and show that Q and $Q^{g^{-1}}$ are conjugate in H .

1D.6. Show that a subgroup of a nilpotent group is maximal if and only if it has prime index.

1D.7. For any finite group G , the **Frattini subgroup** $\Phi(G)$ is the intersection of all maximal subgroups. Show that $\Phi(G)$ is exactly the set of “useless” elements of G , by which we mean the elements $g \in G$ such that if $\langle X \cup \{g\} \rangle = G$ for some subset X of G , then $\langle X \rangle = G$.

1D.8. A finite p -group is **elementary abelian** if it is abelian and every nonidentity element has order p . If G is nilpotent, show that $G/\Phi(G)$ is abelian, and that if G is a p -group, then $G/\Phi(G)$ is elementary abelian.

Note. It is not hard to see that if P is a p -group, then $\Phi(P)$ is the unique normal subgroup of P minimal with the property that the factor group is elementary abelian.

1D.9. If P is a noncyclic p -group, show that $|P : \Phi(P)| \geq p^2$, and deduce that a group of order p^2 must be either cyclic or elementary abelian.

1D.10. Let A be maximal among the abelian normal subgroups of a p -group P . Show that $A = \mathbf{C}_P(A)$, and deduce that $|P : A|$ divides $(|A| - 1)!$.

Hint. Let $C = \mathbf{C}_P(A)$. If $C > A$, apply Lemma 1.23.

1D.11. Let n be the maximum of the orders of the abelian subgroups of a finite group G . Show that $|G|$ divides $n!$.

Hint. Show that for each prime p , the order of a Sylow p -subgroup of G divides $n!$.

Note. There exist infinite groups in which the abelian subgroups have bounded order, so finiteness is essential here.

1D.12. Let p be a prime dividing the order of a group G . Show that the number of elements of order p in G is congruent to -1 modulo p .

1D.13. If $Z \subseteq \mathbf{Z}(G)$ and G/Z is nilpotent, show that G is nilpotent.

1D.14. Show that the Frattini subgroup $\Phi(G)$ of a finite group G is nilpotent.

Hint. Apply the Frattini argument. The proof here is somewhat similar to the proof that (3) implies (4) in Theorem 1.26.

Note. This problem shows that $\Phi(G) \subseteq \mathbf{F}(G)$.

1D.15. Suppose that $\Phi(G) \subseteq N \triangleleft G$ and that $N/\Phi(G)$ is nilpotent. Show that N is nilpotent. In particular, if $G/\Phi(G)$ is nilpotent, then G is nilpotent.

Note. This generalizes the previous problem, which follows by setting $N = \Phi(G)$. Note that this problem proves that $\mathbf{F}(G/\Phi(G)) = \mathbf{F}(G)/\Phi(G)$.

1D.16. Let $N \triangleleft G$, where G is finite. Show that $\Phi(N) \subseteq \Phi(G)$.

Hint. If some maximal subgroup M of G fails to contain $\Phi(N)$, then $\Phi(N)M = G$, and it follows that $N = \Phi(N)(N \cap M)$.

1D.17. Let $N \triangleleft G$, where N is nilpotent and G/N' is nilpotent. Prove that G is nilpotent.

Hint. The derived subgroup N' is contained in $\Phi(N)$ by Problem 1D.8.

Note. If we weakened the assumption that G/N' is nilpotent and assumed instead that G/N is nilpotent, it would not follow that G is necessarily nilpotent.

1D.18. Show that $\mathbf{F}(G/\mathbf{Z}(G)) = \mathbf{F}(G)/\mathbf{Z}(G)$ for all finite groups G .

1D.19. Let $F = \mathbf{F}(G)$, where G is an arbitrary finite group, and let $C = \mathbf{C}_G(F)$. Show that $G/(G \cap F)$ has no nontrivial abelian normal subgroup.

Hint. Observe that $\mathbf{F}(G) \triangleleft G$.

1E

From the earliest days of group theory, researchers have been intrigued by the question: what are the finite simple groups? Of course, the abelian simple groups are exactly the groups of prime order, and (up to isomorphism) there is just one group of order p for each prime p : the cyclic group of that order. But *nonabelian* simple groups are comparatively rare. There are, for example, only five numbers less than 1,000 that occur as orders of nonabelian simple groups, and up to isomorphism, there is just one simple group of each of these orders. (These numbers are 60, 168, 360, 504 and 660.) There do exist numbers, however, such that there are two nonisomorphic simple groups of that order. (The smallest such number is $8!/2 = 20,160$.) But no number is the order of three nonisomorphic simple groups.

Perhaps their rarity is one reason that nonabelian finite simple groups have inspired such intense interest over the years. It seems quite natural to collect rare objects and to attempt to acquire a complete collection. But a more “practical” explanation is that a knowledge of all finite simple groups and their properties would be a major step in understanding *all* finite groups. The reason for this is that, in some sense, all finite groups are built from simple groups.

To be more precise, suppose that G is any nontrivial finite group. By finiteness, G has at least one maximal normal subgroup N . (We mean, of course, a maximal *proper* normal subgroup, but as is customary in this context, we have not made the word “proper” explicit.) Then by the correspondence theorem, the group G/N is simple. (This is because the normal subgroups of G/N are in natural correspondence with the normal subgroups of G that contain N , and there are just two of these: N and G .) Now if N is nontrivial, we can repeat the process by choosing a maximal normal subgroup M of N . (In general, of course, M will not be normal in G .) Because G is finite, we see that if we continue like this, repeatedly choosing a maximal normal subgroup of the previously selected group, we must eventually reach the identity subgroup. If we number our subgroups from the bottom up, we see that we have constructed (or more accurately “chosen”) a chain of subgroups N_i such that

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = G$$

such that each of the factors N_i/N_{i-1} is simple for $1 \leq i \leq r$. In this situation, the subgroups N_i are said to form a **composition series** for G , and the simple groups N_i/N_{i-1} are the corresponding **composition factors**. The Jordan-Hölder theorem asserts that despite the arbitrariness of the construction of the composition series, the set of composition factors (including multiplicities) is uniquely determined up to isomorphism. The

composition factors of G are the simple groups from which we might say that G is constructed. (We mention that the finite groups for which all composition factors are cyclic of prime order are exactly the “solvable” finite groups, which we study in more detail in Chapter 3.)

The problem of finding all nonabelian finite simple groups can be approached from two directions: construct as many simple groups as you can, and prove that every finite nonabelian simple group appears in your list. In particular, as part of the second of these programs, it is useful to prove “nonsimplicity” theorems that show that groups that look different from the known simple groups cannot, in fact, be simple. A major result of this type from early in the 20th century is due to W. Burnside, who showed that the order of a nonabelian simple group must have at least three different prime divisors. (This is Burnside’s classic $p^a q^b$ -theorem.)

Burnside also observed that all of the then known nonabelian simple groups had even order. He conjectured that this holds in general: that all odd-order simple groups are cyclic of prime order. Burnside’s conjecture, which can be paraphrased as the assertion that every group of odd order is solvable, was eventually proved by W. Feit and J. G. Thompson in the early 1960s. (The celebrated Feit-Thompson paper, at about 250 pages, may have been the longest published proof of a single theorem at the time.) Since around 1960, there has been dramatic progress with both aspects of the simple-group-classification problem, and it appears that now, in the early years of the 21st century, the classification of finite simple groups is complete.

So what are the nonabelian finite simple groups? A highly abbreviated description is this. Every finite nonabelian group is either:

- (1) One of the alternating groups A_n for $n \geq 5$,
- (2) A member of one of a number of infinite families parameterized by prime-powers q and (usually) by integers $n \geq 2$, or
- (3) One of 26 other “sporadic” simple groups that do not fit into types (1) or (2).

Of the simple groups in parameterized families, the easiest to describe are the **projective special linear** groups $PSL(n, q)$, where q is a prime-power and $n \geq 2$. These are constructed as follows. Let F be the field of order q and construct the **general linear** group $GL(n, q)$ consisting of all invertible $n \times n$ matrices over F . The **special linear** group $SL(n, q)$ is the normal subgroup of $GL(n, q)$ consisting of those matrices with determinant 1. It is not hard to see that the center $Z = \mathbf{Z}(SL(n, q))$ consists exactly of the scalar matrices of determinant 1, and by definition, $PSL(n, q)$ is the factor group $SL(n, q)/Z$. It turns out that $PSL(n, q)$ is simple except

when $n = 2$ and q is 2 or 3. (We say more about the groups $PSL(n, q)$ in Chapter 7, and we prove their simplicity in Chapter 8, where we also prove that the alternating groups A_n are simple for $n \geq 5$.)

In fact, all of the simple groups with order less than 1,000 are of the form $PSL(2, q)$, where q is one of 5, 7, 8, 9 or 11, and the corresponding group orders are 60, 168, 504, 360 and 660. The unique (up to isomorphism) simple group $PSL(2, 5)$ of order 60 has two other realizations: it is isomorphic to $PSL(2, 4)$ and also to the alternating group A_5 . The simple groups $PSL(2, 7)$ of order 168 and $PSL(2, 9)$ of order 360 also have multiple realizations: the first of these is isomorphic to $PSL(3, 2)$ and the second is isomorphic to A_6 .

The smallest of the 26 sporadic simple groups is the small Mathieu group, denoted M_{11} , of order 7,920; the largest is the Fischer-Griess “monster” of order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 = \\ 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000.$$

For the remainder of this section, we discuss nonsimplicity theorems of the form: “if the order of G is ..., then G cannot be simple”. (Of course, both Burnside’s $p^a q^b$ -theorem and the Feit-Thompson odd-order theorem are of this type.) A very much more elementary result of this form is immediate from the fact that a nontrivial p -group always has a nontrivial center. If $|G|$ is divisible by only one prime, it follows that G cannot be simple unless $Z(G) = G$, and in this case, G is abelian, and so it must be cyclic of prime order.

Burnside’s $p^a q^b$ -theorem asserts that the order of a simple group cannot have exactly two prime divisors. His beautiful (and short) proof is not elementary since it uses character theory (which we do not discuss in this book). It took about 50 years before a purely group-theoretic (and harder) proof of Burnside’s theorem was found by Goldschmidt, Matsuyama and Bender, using powerful techniques of Thompson, Glauberman and others. These techniques were developed for other purposes, and eventually they led to the full classification of finite simple groups, but as a test of their power, it seemed reasonable to see if they would yield a direct proof of Burnside’s theorem. Indeed they did, and one of the goals of this book is to develop enough group theory so that we can present a somewhat simplified version of the Goldschmidt-Matsuyama-Bender proof of Burnside’s theorem. (This proof appears in Chapter 7.)

For now, however, we use Sylow theory (and a few tricks) to prove some much more elementary nonsimplicity theorems.

1.30. Theorem. *Let $|G| = pq$, where $q < p$ are primes. Then G has a normal Sylow p -subgroup. Also, G is cyclic unless q divides $p - 1$.*

Proof. Since $n_p \equiv 1 \pmod{p}$, we see that if $n_p > 1$, we have $n_p > p > q$. This is not possible, however, since n_p must divide q . We conclude that $n_p = 1$, as wanted. Also, since every element of G of order p generates a subgroup of order p , and there is only one of these, there are exactly $p - 1$ elements of order p in G .

Now if $n_q > 1$, then $p = n_q \equiv 1 \pmod{q}$, and thus q divides $p - 1$. Otherwise $n_q = 1$, and we see that there are exactly $q - 1$ elements of order q in G . Together with the identity, we have now accounted for $p + q - 1$ elements of G . But $p + q - 1 < 2p \leq pq = |G|$, and so G must have some element g that does not have order either 1, q or p . Since $o(g)$ divides $|G| = pq$, the only possibility is that $o(g) = pq$, and thus $G = \langle pq \rangle$ is cyclic. ■

1.31. Theorem. *Let $|G| = p^2q$, where p and q are primes. Then G has either a normal Sylow p -subgroup or a normal Sylow q -subgroup.*

Proof. We assume that $n_p > 1$ and $n_q > 1$, and we note that $p \neq q$. Since $n_p \equiv 1 \pmod{p}$, it follows that $n_p > p$ and similarly $n_q > q$.

Now n_p must divide q , and hence $n_p = q$ and we have $n_q > q = n_p > p$. But n_q divides p^2 , and we see that the only possibility is that $n_q = p^2$, which means that G has p^2 subgroups of order q .

If $Q_1 \neq Q_2$ are subgroups of order q , then since q is prime, it follows via Lagrange's theorem that $Q_1 \cap Q_2 = 1$. The p^2 subgroups of order q in G , therefore, have no nonidentity elements in common, and it follows that G has at least $p^2(q - 1)$ elements of order q . (Actually, since every element of order q in G must lie in some subgroup of order q , it follows that G has *exactly* $p^2(q - 1)$ elements of order q , but we shall not need that fact.) The number of elements of G that do not have order q is then at most $|G| - p^2(q - 1) = p^2$. If $P \in \text{Syl}_p(G)$, then, of course, no element of P has order q , and since $|P| = p^2$, it follows that P is exactly equal to the set of elements of G that do not have order q . In particular, P is uniquely determined, and this is a contradiction since we are assuming that $n_p > 1$. ■

By the previous two theorems, we see that if $p \neq q$ are primes, then a group of order pq or of order p^2q must either have a normal Sylow p -subgroup or a normal Sylow q -subgroup. This almost works for groups of order p^3q too, but there is an exception. This situation is endemic in finite group theory: some general fact holds with a small number of exceptions.

(Another example of this phenomenon is that all automorphisms of the symmetric group S_n are inner for all integers $n \geq 1$ except $n = 6$.)

1.32. Theorem. *Let $|G| = p^3q$, where p and q are primes. Then G has either a normal Sylow p -subgroup or a normal Sylow q -subgroup, except when $|G| = 24$.*

Proof. As in the previous proof, we assume that $n_p > 1$ and that $n_q > 1$, and we conclude that $p \neq q$ and that $n_p > p$ and $n_q > q$. Continuing to reason as we did previously, we have $n_q > q = n_p > p$. Since n_q divides p^3 , we are left this time with two possibilities: either $n_q = p^3$ or $n_q = p^2$.

Suppose that $n_q = p^3$. Then the p^3 subgroups of order q contain a total of $p^3(q-1)$ elements of order q , and thus G contains at most $|G| - p^3(q-1) = p^3$ elements that do not have order q . It follows that if $P \in \text{Syl}_p(G)$, then P is exactly the set of elements of G having order different from q , and thus P is unique, contradicting the assumption that $n_p > 1$.

We conclude, therefore, that $n_q = p^2$, and thus $p^2 \equiv 1 \pmod{q}$. In other words, q divides $p^2 - 1 = (p+1)(p-1)$. Since q is prime, we see that q must divide either $p+1$ or $p-1$, and so in either case, we have $q \leq p+1$. But we know from the first paragraph of the proof that $p < q$, and so the only possibility is that $q = p+1$. Now p and q are primes that differ by 1, and so one of them must be even. We deduce that $p = 2$ and $q = 3$, and thus $|G| = 24$. ■

Of course, the previous proof does not tell us that there actually is an exception of order 24; it only permits the possibility of such an exception. But an exception really does exist. Consider S_4 , the symmetric group on four symbols, which, of course, has order $4! = 24$. By examining the possible cycle structures for elements of S_4 , it is easy to count that there are exactly nine elements of order 2, eight elements of order 3 and six elements of order 4. (As a check, note that $9+8+6 = 23$, so that together with the identity, we have accounted for all 24 elements.) By the Sylow D-theorem, every element of 2-power order in S_4 lies in some Sylow 2-subgroup. Since each Sylow 2-subgroup has order 8, and yet there are more than eight elements of 2-power order, it follows that S_4 must have more than one Sylow 2-subgroup. Similar reasoning shows that there must be more than one Sylow 3-subgroup. (In fact, it is easy to see that $n_2(S_4) = 3$ and that $n_3(S_4) = 4$.)

There is still more that we can say about this situation. We know that among groups of order p^3q , only groups of order 24 can fail to have a nontrivial normal Sylow subgroup, and we know that at least one group of order 24 actually does fail to have such a Sylow subgroup. The remaining question is whether or not there are any other groups of order 24 that can occur as exceptions. The answer is “no”.

1.33. Theorem. *Let $|G| = 24$, and suppose $n_2(G) > 1$ and $n_3(G) > 1$. Then $G \cong S_4$.*

Proof. Since n_3 exceeds 1, is congruent to 1 modulo 3 and divides 8, the only possibility is that $n_3 = 4$, and thus $|G : N| = 4$, where $N = \mathbf{N}_G(P)$ and $P \in \text{Syl}_3(G)$. Now let $K = \text{core}_G(N)$, so that G/K is isomorphic to a subgroup of S_4 by Theorem 1.1. It suffices to show that $K = 1$ since that will imply that G is isomorphic to a subgroup of S_4 , and this will complete the proof since $|G| = 24 = |S_4|$.

Recall that $K \subseteq N = \mathbf{N}_G(P)$, where $P \in \text{Syl}_3(G)$. Then P is a normal Sylow 3-subgroup of KP , and so P is characteristic in KP . Since P is not normal in G , however, we conclude that KP cannot be normal in G . But KP/K is a Sylow 3-subgroup of G/K , and it follows that $n_3(G/K) > 1$. In particular, G/K is not a 2-group, and so $|K|$ is not divisible by 3.

Since $|G : N| = 4$, we see that $|N| = 6$, and hence the only possibilities are $|K| = 1$, as wanted, or $|K| = 2$. Assuming now that $|K| = 2$, we work to obtain a contradiction. Since $|G/K| = 12$, Theorem 1.31 applies, and we deduce that either $n_2(G/K) = 1$ or $n_3(G/K) = 1$. Since we have seen that $n_3(G/K) > 1$, however, we conclude that G/K has a unique Sylow 2-subgroup S/K . Then $S/K \triangleleft G/K$, and so $S \triangleleft G$. Also $|S| = 8$ since $|K| = 2$ and $|S/K| = 4$, and thus S is a normal Sylow 2-subgroup of G . This contradicts the hypothesis that $n_2(G) > 1$. ■

We mention that the group S_4 , of order 24, is not simple, and it follows that no group of order p^3q is simple, where p and q are primes. In fact, S_4 has a normal subgroup of order 12 and one of order 4. The subgroup of order 12 is the alternating group A_4 (see the discussion below) and the normal subgroup of order 4 is the so-called **Klein group** consisting of the identity and the three elements of order 2 in S_4 that have no fixed points.

We can eliminate a quarter of all positive integers as possibilities for the order of a simple group. The argument relies on the notion of odd and even permutations, with which, we assume the reader is familiar.

Briefly, the facts are these. Every permutation of a finite set can be written as a product of transpositions (2-cycles). A permutation that can be written as a product of an even number of transpositions is **even** and one that can be written as a product of an odd number of transpositions is **odd**. It is a triviality that the even permutations in the symmetric group S_n form a subgroup. (It is called the **alternating group** and is denoted A_n .) It is also true, but much less trivial to prove, that no permutation can be both even and odd, and since odd permutations certainly exist for $n \geq 2$, we see that A_n is proper in S_n in this case.

More generally, suppose that G is an arbitrary group that acts on some finite set Ω , and assume that there is at least one element $x \in G$ that induces an odd permutation on Ω . It should be clear that the elements of G that induce even permutations on Ω form a subgroup, which we call H . Since $x \notin H$, we see that $H < G$, and we claim that $|G : H| = 2$. To see this, it suffices to show that the set $G - H$ is contained in a single right coset of H . We show, in fact, that if $g \in G - H$, then $g \in Hx^{-1}$. Now g induces an odd permutation on Ω , and hence gx induces an even permutation and we have $gx \in H$. Then $g \in Hx^{-1}$, as claimed. Since a subgroup of index 2 is automatically normal, we have established the following useful fact.

1.34. Lemma. *Let G act on a finite set Ω and suppose that some element of G acts “oddly”. Then G has a normal subgroup of index 2. ■*

1.35. Theorem. *Suppose that $|G| = 2n$, where n is odd. Then G has a normal subgroup of index 2.*

Proof. By Cauchy’s theorem, we can find an element $t \in G$ of order 2. In the regular action of G on itself by right multiplication, t has no fixed points, and so the permutation induced by t consists entirely of 2-cycles, and there are $|G|/2 = n$ of them. Since n is odd, the permutation induced by t is odd, and the result follows by Lemma 1.34. ■

We have stated that 60 is the smallest number that occurs as the order of a nonabelian simple group. In fact, using what we have now proved, this is not very hard to see. First, we can eliminate all powers of primes since if G is a simple p -group, then because $1 < \mathbf{Z}(G) \triangleleft G$, we see that $\mathbf{Z}(G) = G$ and G is abelian. Also, by Theorem 1.30, we can eliminate all products of two primes, and thus we can assume that $|G|$ factors as a product of at least three primes, counting multiplicity.

Suppose now that $|G| < 60$ and write $n = |G|$. If n is odd, then, since 3^4 , $3^2 \cdot 7$ and $3 \cdot 5^2$ all exceed 60, we see that the only possibilities that are products of at least three primes are $n = 3^3$ and $n = 3^2 \cdot 5$, and we have seen that neither of these numbers can be the order of a simple group.

We are left with the cases where n is even. By Theorem 1.35, we can suppose that n is divisible by 4, and we write $n = 4m$, where $m < 15$. We have eliminated the cases where m is prime or is a power of 2, and also the cases where $m = 2p$, where p is an odd prime. The the only surviving possibilities for m are 9 and 12, and so we need to show that there is no simple group of order 36 or of order 48.

If G is simple of order $36 = 2^2 \cdot 3^2$, we see that $|G : P| = 4$, where $P \in \text{Syl}_3(G)$, and yet $|G : P|$ does not divide $4! = 24$. This violates the $n!$ -theorem, Corollary 1.3. Similarly, if $|G| = 48 = 2^4 \cdot 3$, we get a violation of

the $n!$ -theorem by taking $P \in \text{Syl}_2(G)$, so that $|G : P| = 3$. This completes the proof that 60 is the smallest possible order of a nonabelian simple group.

To prove that no number between 60 and 168 can be the order of a simple group, it is convenient to have two more nonsimplicity results of the type we have been discussing: if G has order p^2q^2 or order pqr , where p , q and r are primes, then G cannot be simple. (We leave the proofs of these to the exercises at the end of this section.) Using these two facts and the other results that we have established, all but about a dozen of the numbers between 60 and 168 can be eliminated, and most of those are easily dealt with by *ad hoc* methods. For example, we need to consider the numbers $84 = 2^2 \cdot 3 \cdot 7$, $140 = 2^2 \cdot 5 \cdot 7$ and $156 = 2^2 \cdot 3 \cdot 13$, and these are easily eliminated by the observation that if p is the largest prime divisor, then $n_p = 1$ since no divisor of n exceeding 1 is congruent to 1 modulo p .

The number $72 = 2^3 \cdot 3^2$ can be eliminated by observing that if G is simple and $|G| = 72$, then $n_3 > 1$, and therefore the only possibility is $n_3 = 4$. Then $|G : N| = 4$, where N is the normalizer of a Sylow 3-subgroup, and this violates the $n!$ -theorem. More interesting is the case where $|G| = 144 = 2^4 \cdot 3^2$. This case can be handled using Theorem 1.16, with an argument analogous to the one we used in the discussion following Corollary 1.17, where we showed that groups of order $2^6 \cdot 7^3$ are not simple. Another number that requires some work is $132 = 2^2 \cdot 3 \cdot 11$. If a group of this order is simple, then $n_{11} = 12$, and hence there are at least 120 elements of order 11, leaving at most 12 other elements. It follows that $n_3 = 4$, and this yields a contradiction using the $n!$ -theorem.

The number between 60 and 168 that seems to be the most difficult to eliminate is $120 = 2^3 \cdot 3 \cdot 5$. One (rather tricky) approach is this. If G is simple of order 120, it is easy to see that $n_5(G) = 6$. Then G acts (nontrivially) on the six right cosets of the normalizer of a Sylow 5-subgroup, and this determines a nontrivial homomorphism from G into the symmetric group S_6 . Since G is simple, this homomorphism is injective, and thus there is an isomorphic copy H of G with $H \subseteq S_6$. But G has no normal subgroup of index 2, and hence by Lemma 1.34, no element of G can act oddly on the six cosets, and thus H actually lies in the alternating group A_6 , and since $|A_6| = 360$, we see that $|A_6 : H| = 3$. Recall, however, that the alternating groups A_n are simple when $n \geq 5$, and so by the $n!$ -theorem, A_6 cannot have a subgroup of index 3. This contradiction shows that 120 is not the order of a simple group.

An alternative approach for eliminating 120 is to quote Problem 1C.4, which asserts that if $|G| = 120$, then there exists a subgroup $H \subseteq G$ with $1 < |G : H| \leq 5$. If G is simple, this yields an isomorphism of G into the symmetric group S_5 . Since $|S_5| = 120 = |G|$, we conclude that $G \cong S_5$,

and this is a contradiction since S_5 has a normal subgroup of index 2: the alternating group A_5 .

We close this section with one further result which, though somewhat more general than those that we have already proved, is still only a very special case of Burnside's $p^a q^b$ -theorem.

1.36. Theorem. *Suppose that $|G| = p^a q$, where p and q are primes and $a > 0$. Then G is not simple.*

Proof. We can certainly assume that $p \neq q$ and that $n_p > 1$, and thus $n_p = q$. Now choose distinct Sylow p -subgroups S and T of G such that $|S \cap T|$ is as large as possible, and write $D = S \cap T$.

If $D = 1$, then every pair of distinct Sylow p -subgroups of G intersect trivially, and so the Sylow p -subgroups of G account for a total of $q(p^a - 1)$ nonidentity elements of G . All of these elements, of course, have orders divisible by p , and this leaves room for at most $|G| - q(p^a - 1) = q$ elements with order not divisible by p . It follows that if $Q \in \text{Syl}_q(G)$, then Q is exactly the set of these elements, and in particular Q is unique, and so $Q \triangleleft G$ and G is not simple, as required.

We can now assume that $D > 1$, and we let $N = \mathbf{N}_G(D)$. Since $D < S$ and $D < T$ and we know that “normalizers grow” in p -groups, we can conclude that $N \cap S > D$ and $N \cap T > D$.

Next, we show that N is not a p -group. Otherwise, by the Sylow D -theorem, we can write $N \subseteq R \in \text{Syl}_p(G)$. Then $R \cap S \supseteq N \cap S > D$, and so by the choice of D , we see that the Sylow subgroups R and S cannot be distinct. In other words, $S = R$ and similarly, $T = R$. But this is a contradiction since $S \neq T$.

It follows that q divides $|N|$, and so if we choose $Q \in \text{Syl}_q(N)$, we have $|Q| = q$. Now S is a p -group and Q is a q -group, and thus $S \cap Q = 1$ and we have $|SQ| = |S||Q| = p^a q = |G|$. Then $SQ = G$, and hence if $g \in G$ is arbitrary, we can write $g = xy$, where $x \in S$ and $y \in Q$. Then $S^g = S^{xy} = S^y \supseteq D^y = D$, where the second equality holds since $x \in S$ and the last equality follows because $y \in Q \subseteq N = \mathbf{N}_G(D)$. We see, therefore, that D is contained in every conjugate of S in G . Then D is contained in every Sylow p -subgroup of G , and we have $1 < D \subseteq \mathbf{O}_p(G)$. Thus $\mathbf{O}_p(G)$ is a nonidentity proper normal subgroup G , and this completes the proof that G is not simple. ■

Problems 1E

1E.1. Let $|G| = p^2 q^2$, where $p < q$ are primes. Prove that $n_q(G) = 1$ unless $|G| = 36$.

Note. If $|G| = 36$, then a Sylow 3 subgroup really can fail to be normal, but in that case, one can show that a Sylow 2-subgroup of G is normal.

1E.2. Let $|G| = pqr$, where $p < q < r$ are primes. Show that $n_r(G) = 1$.

Hint. Otherwise, show by counting elements that a Sylow q -subgroup must be normal and consider the factor group, of order pr .

Note. In general, if $|G|$ is a product of distinct primes, then a Sylow subgroup for the largest prime divisor of $|G|$ is normal. We prove this theorem of Burnside when we study transfer theory in Chapter 5.

1E.3. Show that there is no simple group of order $315 = 3^2 \cdot 5 \cdot 7$.

Note. This, of course, is also a consequence of the Feit-Thompson odd-order theorem, which asserts that no group of odd nonprime order can be simple.

1E.4. If $|G| = 144 = 2^4 \cdot 3^2$, show that G is not simple.

1E.5. If $|G| = 336 = 2^4 \cdot 3 \cdot 7$, show that G is not simple.

Hint. If G is simple, compute $n_7(G)$ and use Problem 1C.5.

1E.6. If $|G| = 180 = 2^2 \cdot 3^2 \cdot 5$, show that G is not simple.

1E.7. If $|G| = 240 = 2^4 \cdot 3 \cdot 5$, show that G is not simple.

1E.8. If $|G| = 252 = 2^2 \cdot 3^2 \cdot 7$, show that G is not simple.

1F

Recall that $\mathbf{O}_p(G)$ is the unique largest normal p -subgroup of the finite group G , and that it can be found by taking the intersection of all of the Sylow p -subgroups of G . But do we really need all of them? What is the smallest collection of Sylow p -subgroups of G with the property that their intersection is $\mathbf{O}_p(G)$? In the case where a Sylow p -subgroup is abelian, there is a pretty answer, which was found by J. S. Brodkey. (Of course, since the Sylow p -subgroups of G are conjugate by Sylow C-theorem, they are isomorphic, and so if any one of them is abelian, they all are.)

1.37. Theorem (Brodkey). *Suppose that a Sylow p -subgroup of a finite group G is abelian. Then there exist $S, T \in \text{Syl}_p(G)$ such that $S \cap T = \mathbf{O}_p(G)$.*

Of course, every intersection of two Sylow p -subgroups of G contains $\mathbf{O}_p(G)$, so what Brodkey's theorem really says is that if the Sylow subgroups are abelian, then $\mathbf{O}_p(G)$ is the unique minimal such intersection. In fact, what is essentially Brodkey's argument establishes something about minimal intersections of two Sylow p -subgroups even if the Sylow subgroups are not abelian.

1.38. Theorem. Fix a prime p , and let G be any finite group. Choose $S, T \in \text{Syl}_p(G)$ such that $D = S \cap T$ is minimal in the set of intersections of two Sylow p -subgroups of G . Then $\mathbf{O}_p(G)$ is the unique largest subgroup of D that is normal in both S and T .

If we assume that S and T are abelian in Theorem 1.38, we see that $D \triangleleft S$ and $D \triangleleft T$, and so in this case, the theorem guarantees that $D = \mathbf{O}_p(G)$. In other words, Brodkey's theorem is an immediate corollary of Theorem 1.38.

Proof of Theorem 1.38. Let $K \subseteq D$, where $K \triangleleft S$ and $K \triangleleft T$. We must show that $K \subseteq \mathbf{O}_p(G)$, or equivalently, that $K \subseteq P$ for all Sylow p -subgroups P of G .

Let $N = \mathbf{N}_G(K)$ and note that $S \subseteq N$, and thus $S \in \text{Syl}_p(N)$. Now let $P \in \text{Syl}_p(G)$ and observe that $P \cap N$ is a p -subgroup of N . Then $P \cap N$ is contained in some Sylow p -subgroup of N , and so we can write $P \cap N \subseteq S^x$ for some element $x \in N$. (We are, of course, using the Sylow D- and C-theorems in the group N .) Now $T \subseteq N$, and thus also $T^x \subseteq N$ and we have

$$P \cap T^x = P \cap N \cap T^x \subseteq S^x \cap T^x = D^x.$$

Then

$$D = (D^x)^{x^{-1}} \supseteq (P \cap T^x)^{x^{-1}} = P^{x^{-1}} \cap T.$$

Since $P^{x^{-1}}$ and T are Sylow p -subgroups of G , and their intersection is contained in D , it follows by the minimality of D that $P^{x^{-1}} \cap T = D$. In particular, we have $K \subseteq D \subseteq P^{x^{-1}}$, and thus $K^x \subseteq P$. But $K^x = K$ since $x \in N = \mathbf{N}_G(K)$, and thus $K \subseteq P$, as required. ■

1.39. Corollary. Let $P \in \text{Syl}_p(G)$, where G is a finite group, and assume that P is abelian. Then $|G : \mathbf{O}_p(G)| \leq |G : P|^2$.

Proof. By Brodkey's theorem, we can choose $S, T \in \text{Syl}_p(G)$ such that $S \cap T = \mathbf{O}_p(G)$. Then

$$|G| \geq |ST| = \frac{|S||T|}{|S \cap T|} = \frac{|P|^2}{|\mathbf{O}_p(G)|}.$$

This yields $|G|/|P|^2 \geq 1/|\mathbf{O}_p(G)|$, and the result follows by multiplying both sides of this inequality by $|G|$. ■

We can recast this as a “good” nonsimplicity theorem.

1.40. Corollary. Let $P \in \text{Syl}_p(G)$, where G is finite and P is abelian, and assume that $|P| > |G|^{1/2}$. Then $\mathbf{O}_p(G) > 1$, and thus G is not simple unless $|G| = p$.

Proof. We have $|G : P|^2 = |G|^2/|P|^2 < |G|$, and thus $\mathbf{O}_p(G) > 1$ by Corollary 1.39. ■

We mention that the conclusion of Brodkey's theorem definitely can fail if the Sylow p -subgroups are nonabelian. A counterexample is a certain group G of order $144 = 2^4 \cdot 3^2$ for which $\mathbf{O}_2(G) = 1$. Taking $p = 2$, we see that the conclusion of Corollary 1.40 fails for this group, and thus the conclusion of Brodkey's theorem must also fail. Of course, the Sylow 2-subgroups of G are necessarily nonabelian in this case.

This counterexample of order 144 can be constructed as follows. Let E be elementary abelian of order 9. (In other words, E is the direct product of two cyclic groups of order 3.) Then E can be viewed as a 2-dimensional vector space over a field of order 3, and thus the full automorphism group of E is isomorphic to $GL(2, 3)$, which has order 48. A Sylow 2-subgroup T of this automorphism group, therefore, has order 16, and of course, since $T \subseteq \text{Aut}(E)$, we see that T acts on E and that this action is faithful.

Using the “semidirect product” construction, which we discuss in Chapter 3, we can build a group G containing (isomorphic copies of) E and T , where $E \triangleleft G = ET$, and the conjugation action of T on E within G is identical to the original faithful action of T on E . Now $\mathbf{O}_2(G) \triangleleft G$ and $E \triangleleft G$, and since $\mathbf{O}_2(G)$ is a 2-group and E is a 3-group, we see that $\mathbf{O}_2(G) \cap E = 1$. It follows that $\mathbf{O}_2(G)$ centralizes E , and thus $\mathbf{O}_2(G)$ is contained in the kernel of the conjugation action of T on E . This action is faithful, however, and we deduce that $\mathbf{O}_2(G) = 1$, and indeed we have a counterexample.

Problems 1F

1F.1. In the last paragraph of this section, we used the fact that if $M \triangleleft G$ and $N \triangleleft G$ and $M \cap N = 1$, then M and N centralize each other. Prove this.

Hint. Consider elements of the form $m^{-1}n^{-1}mn$, where $m \in M$ and $n \in N$.

Note. Recall that if $x, y \in G$, then the element $x^{-1}y^{-1}xy \in G$ is the **commutator** of x and y . It is customary to write $[x, y]$ to denote this element. Note that $[x, y] = 1$ if and only if $xy = yx$. We study commutators in more detail in Chapter 4.

1F.2. Let G be a group, and fix a prime p . Show that if $\mathbf{O}_p(G) = 1$, then there exist $S, T \in \text{Syl}_p(G)$ such that $\mathbf{Z}(S) \cap \mathbf{Z}(T) = 1$.

1F.3. Let $G = NP$, where $N \triangleleft G$, $P \in \text{Syl}_p(G)$ and $N \cap P = 1$, and assume that the conjugation action of P on N is faithful. Show that P acts faithfully on at least one orbit of this action.

Hint. In fact, if $x \in N$ is chosen so that $|P \cap P^x|$ is as small as possible, then P acts faithfully on the P -orbit containing x .

1G

Suppose that $A \subseteq G$ is an abelian subgroup, and that the index $n = |G : A|$ is relatively small. Can we conclude that G has a *normal* abelian subgroup N such that the index $|G : N|$ is under control? Yes, certainly; we know that $|G : \text{core}_G(A)| \leq n!$, and of course, $\text{core}_G(A)$ is normal, and since this subgroup is contained in A , it is abelian.

A bound much better than $|G : N| \leq n!$ is available if the abelian subgroup A happens to be a Sylow subgroup of G . Assuming that A is a Sylow p -subgroup, we can take $N = \mathbf{O}_p(G)$, and then Corollary 1.39 tells us that $|G : N| \leq n^2$. Surprisingly, it is not necessary to assume that A is a Sylow subgroup; there *always* exists an abelian normal subgroup N with $|G : N| \leq n^2$. Although this remarkable theorem of A. Chermak and A. Delgado does not depend on Sylow theory, it seems appropriate to include it here since it can be viewed as a generalization of Corollary 1.39.

1.41. Theorem (Chermak-Delgado). *Let G be a finite group. Then G has a characteristic abelian subgroup N such that $|G : N| \leq |G : A|^2$ for every abelian subgroup $A \subseteq G$.*

As we shall see, the key idea in the proof of the Chermak-Delgado theorem is very elementary. But it is powerful, and it yields even more than we stated in Theorem 1.41. The trick is to define the integer $m_G(H) = |H||\mathbf{C}_G(H)|$ for arbitrary subgroups H of a finite group G , and to consider subgroups $H \subseteq G$ where this **Chermak-Delgado measure** is maximized.

We begin with a trivial observation.

1.42. Lemma. *Let $H \subseteq G$, where G is a finite group, and write $C = \mathbf{C}_G(H)$. Then $m_G(H) \leq m_G(C)$ and if equality occurs, then $H = \mathbf{C}_G(C)$.*

Proof. Since $H \subseteq \mathbf{C}_G(C)$, we see that

$$m_G(C) = |C||\mathbf{C}_G(C)| \geq |C||H| = m_G(H),$$

and the result follows. ■

Next, we consider two subgroups simultaneously.

1.43. Lemma. *Let H and K be subgroups of a finite group G , and write $D = H \cap K$ and $J = \langle H, K \rangle$. Then*

$$m_G(H)m_G(K) \leq m_G(D)m_G(J)$$

and if equality holds, then $J = HK$ and $\mathbf{C}_G(D) = \mathbf{C}_G(H)\mathbf{C}_G(K)$.

Proof. Write C_H , C_K , C_D and C_J to denote the centralizers in G of H , K , D and J , respectively, and note that $C_J = C_H \cap C_K$ and that $C_H, C_K \subseteq C_D$. Then

$$|J| \geq |HK| = \frac{|H||K|}{|D|} \quad \text{and}$$

$$|C_D| \geq |C_H C_K| = \frac{|C_H||C_K|}{|C_J|},$$

and it follows that

$$m_G(D) = |D||C_D| \geq \frac{|H||K|}{|J|} \frac{|C_H||C_K|}{|C_J|} = \frac{m_G(H)m_G(K)}{m_G(J)},$$

which establishes the inequality. If equality occurs, then $|J| = |HK|$ and $|C_D| = |C_H C_K|$, and thus $J = HK$ and $G_D = C_H C_K$, as required. ■

We mention that if $H, K \subseteq G$ are subgroups, then the subgroup $J = \langle H, K \rangle$ is often called the **join** of H and K . Also, a collection \mathcal{L} of subgroups of a group G is said to be a **lattice** of subgroups if it is closed under intersections and joins.

1.44. Theorem. *Given a finite group G , let $\mathcal{L} = \mathcal{L}(G)$ be the collection of subgroups of G for which the Chermak-Delgado measure is as large as possible. Then*

- (a) \mathcal{L} is a lattice of subgroups of G .
- (b) If $H, K \in \mathcal{L}$, then $\langle H, K \rangle = HK$.
- (c) If $H \in \mathcal{L}$, then $\mathbf{C}_G(H) \in \mathcal{L}$ and $\mathbf{C}_G(\mathbf{C}_G(H)) = H$.

Proof. Let m be the maximum of the Chermak-Delgado measures of the subgroups of G , and let $H, K \in \mathcal{L}$. Then $m_G(H) = m = m_G(K)$, and so by Lemma 1.43, we have $m^2 = m_G(H)m_G(K) \leq m_G(D)m_G(J)$, where $D = H \cap K$ and $J = \langle H, K \rangle$. But $m_G(D) \leq m$ and $m_G(J) \leq m$ by the maximality of m , and thus $m_G(D) = m = m_G(J)$, and hence D and J lie in \mathcal{L} , as required. Also, since equality holds in Lemma 1.43, we know that $HK = J$, and this proves (b). Finally, statement (c) follows because the maximality of $m_G(H)$ forces equality in Lemma 1.42. ■

1.45. Corollary. *Every finite group G contains a unique subgroup M , minimal with the property that $m_G(M)$ is the maximum of the Chermak-Delgado measures of the subgroups of G . Also M is abelian and $M \supseteq \mathbf{Z}(G)$.*

Proof. Since $\mathcal{L} = \mathcal{L}(G)$ is a lattice, the intersection of all of its members lies in \mathcal{L} , and this is the desired subgroup M . Also, since $M \in \mathcal{L}$, we know that $\mathbf{C}_G(M) \in \mathcal{L}$, and thus $M \subseteq \mathbf{C}_G(M)$, and it follows that M is abelian. Finally, $M = \mathbf{C}_G(\mathbf{C}_G(M)) \supseteq \mathbf{Z}(G)$, and the proof is complete. ■

We shall refer to the subgroup M of Corollary 1.39 as the **Chermak-Delgado** subgroup of G . It is, of course, characteristic in G .

Proof of Theorem 1.41. Since the Chermak-Delgado subgroup M is characteristic and abelian, it suffices to show that $|G : M| \leq |G : A|^2$ for all abelian subgroups $A \subseteq G$. By the definition of M , we have $m_G(M) \geq m_G(A) = |A||C_G(A)| \geq |A|^2$, where the last inequality holds because A is abelian. Then

$$|G : A|^2 = \frac{|G|^2}{|A|^2} \geq \frac{|G|^2}{m_G(M)} = \frac{|G|}{|M|} \frac{|G|}{|C_G(M)|} \geq \frac{|G|}{|M|} = |G : M|,$$

as required.

Another application of the Chermak-Delgado subgroup is the following.

1.46. Corollary. *Let H be a subgroup of a finite group G , and assume that $|H||C_G(H)| > |G|$. Then G is not a nonabelian simple group.*

Proof. Let M be the Chermak-Delgado subgroup of G and observe that $m_G(M) \geq m_G(H) > |G|$. But the Chermak-Delgado measure of the identity subgroup is equal to $|G|$, and it follows that $M > 1$. Since M is abelian and normal in G , the result follows. ■

Problems 1G

1G.1. Let $A \subseteq G$, where A is abelian, and assume that there does not exist a characteristic abelian subgroup N of G such that $|G : N| < |G : A|^2$. Show that $A = C_G(A)$ is a member of the maximum-measure lattice $\mathcal{L}(G)$ and that $|G : \mathbf{Z}(G)| = |G : A|^2$.

1G.2. Let $\mathcal{L}(G)$ be the maximum-measure lattice as in Theorem 1.44, and suppose that $H \in \mathcal{L}(G)$ and that $H < G$. Show that there exists a normal subgroup M of G such that $H \subseteq M < G$.

Hint. Observe that all conjugates of H in G lie in $\mathcal{L}(G)$ and thus the product of any two of them is a subgroup. If H is not contained in a proper normal subgroup of G , show that it is possible to write $G = HK$, where $K < G$ and K contains a conjugate of H . Deduce a contradiction from this.

1G.3. Let G be simple and suppose that $H \subseteq G$ and that $|H||C_G(H)| = |G|$. Show that $H = 1$ or $H = G$.

Hint. If G is nonabelian, show that $H \in \mathcal{L}(G)$.

1G.4. Let $A \subseteq G$, where A is abelian and G is nonabelian. Show that there exists a normal abelian subgroup N of G such that $|G : N| < |G : A|^2$.

Subnormality

2A

We know that in general, normality is not a transitive relation on the set of subgroups of a group. In other words, if $K \triangleleft H$ and $H \triangleleft G$, we cannot usually conclude that $K \triangleleft G$. Following Wielandt, who developed much of the theory that we discuss in this chapter, we “repair” this lack of transitivity by defining a new relation. A subgroup $S \subseteq G$ is said to be **subnormal** in G if there exist subgroups H_i of G such that

$$S = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G,$$

and in this situation, we write $S \triangleleft\triangleleft G$. Subnormality, therefore, is a transitive relation that extends the notion of normality. We stress that the chain of subgroups H_i extending from S up to G is required to be finite, even if G is an infinite group. Note that although we have not required that the subgroups H_i are all distinct, it is always possible to delete repeated groups and to assume that $H_0 < H_1 < \cdots < H_r$.

Of course, if $S \triangleleft\triangleleft G$, there may be a number of different chains of subgroups $\{H_i\}$ that realize the subnormality. The length of the shortest possible chain, or equivalently the smallest possible integer r , is called the **subnormal depth** of S . Thus the whole group G has depth 0 in G ; proper normal subgroups have depth 1, and subnormal subgroups that are not actually normal have depth exceeding 1.

Although we are concerned almost exclusively with finite groups in this book, it should be noted that part of the subnormality theory that we present also works for infinite groups. Some of the theorems that we prove by induction on the group order can also be proved by induction on the subnormal

depth, and most of those results hold for infinite groups too. But the reader should be cautioned that many of the more interesting theorems about subnormality are simply false for general infinite groups.

We begin with a situation where subnormality arises naturally.

2.1. Lemma. *Let G be finite. Then G is nilpotent if and only if every subgroup of G is subnormal.*

Proof. By Theorem 1.26, a finite group is nilpotent if and only if normalizers grow. In other words, G is nilpotent if and only if $H < \mathbf{N}_G(H)$ whenever $H < G$. Now if $H < G$ and H is subnormal, we can write $H = H_0 \triangleleft \cdots \triangleleft H_r = G$, where $r > 0$, and we can assume that $H_1 > H_0$. Since $H = H_0 \triangleleft H_1$, we have $H < H_1 \subseteq \mathbf{N}_G(H)$, and this shows that if every subgroup of G is subnormal, then normalizers grow, and hence G is nilpotent.

Conversely, suppose that G is nilpotent, so that normalizers grow in G . Given $H \subseteq G$, we prove that $H \triangleleft\triangleleft G$ by induction on the index $|G : H|$. If this index is 1, then $H = G$, and H is certainly subnormal. Otherwise, $H < G$, and we have $H < \mathbf{N}_G(H)$. Then $|G : \mathbf{N}_G(H)| < |G : H|$, and so by the inductive hypothesis, $\mathbf{N}_G(H) \triangleleft\triangleleft G$. The result now follows since $H \triangleleft \mathbf{N}_G(H)$. ■

If we wanted to prove that a subgroup S of G is subnormal by using the definition, we would need to construct a chain of subgroups running from S up to G , where each of these subgroups is normal in the next. In the second half of the proof of Lemma 2.1, we found such a chain by being greedy. By this, we mean that in going from H_i to H_{i+1} , we went as far as possible: we took H_{i+1} to be the full normalizer of H_i in G . But greediness does not always yield success. In the symmetric group S_4 , for example, consider any subgroup S of order 2 in the normal Klein subgroup K of order 4. (Recall that the nonidentity elements of K are exactly the permutations in S_4 that are products of two disjoint 2-cycles.) Since K is abelian, we have $S \triangleleft K$, and since $K \triangleleft S_4$, we see that $S \triangleleft\triangleleft S_4$. It is not hard to see, however, that $\mathbf{N}_{S_4}(S)$ has order 8; it is a Sylow 2-subgroup of S_4 . Also, since this Sylow subgroup has index 3 and is not normal, it follows that it is its own normalizer. In other words, we are stuck. We can not continue to construct a subnormal chain from $\mathbf{N}_G(S)$ to G , and so greediness does not work in this case.

We pursue the connection between nilpotence and subnormality a bit further. Recall that the Fitting subgroup $\mathbf{F}(G)$ of a finite group G is the unique largest normal nilpotent subgroup of G . The following result shows that not only does $\mathbf{F}(G)$ contain all normal nilpotent subgroups of G ; it also contains all subnormal nilpotent subgroups.

2.2. Theorem. *Let $H \subseteq G$, where G is finite. Then $H \subseteq \mathbf{F}(G)$ if and only if H is nilpotent and subnormal in G .*

Proof. If $H \subseteq \mathbf{F}(G)$, then of course H is nilpotent since $\mathbf{F}(G)$ is nilpotent. Also, we see by Lemma 2.1 that $H \triangleleft\triangleleft \mathbf{F}(G) \triangleleft G$, and thus $H \triangleleft\triangleleft G$, as wanted.

Conversely, assume that $H \triangleleft\triangleleft G$ and that H is nilpotent. We proceed by induction on $|G|$ to show that $H \subseteq \mathbf{F}(G)$. If $H = G$, then G is nilpotent, and so $H = G = \mathbf{F}(G)$, and we are done in this case. We can assume, therefore, that $H < G$, and we let M be the penultimate term in a subnormal chain of distinct subgroups climbing from H to G . Then $H \triangleleft\triangleleft M \triangleleft G$ and $M < G$. By the inductive hypothesis applied in M , therefore, we have $H \subseteq \mathbf{F}(M)$. But $\mathbf{F}(M)$ is characteristic in M , which is normal in G , and hence $\mathbf{F}(M)$ is a normal nilpotent subgroup of G . This yields $H \subseteq \mathbf{F}(M) \subseteq \mathbf{F}(G)$, as required. ■

We leave nilpotent subgroups for a while to study subnormality more generally. We begin with a basic (and trivial) fact.

2.3. Lemma. *Let $S \triangleleft\triangleleft G$, where G is a group, and suppose that $K \subseteq G$ is an arbitrary subgroup. Then $S \cap K \triangleleft\triangleleft K$.*

Proof. Since S is subnormal in G , there exist subgroups $H_i \subseteq G$ for $0 \leq i \leq r$, where $H_{i-1} \triangleleft H_i$ for $0 < i \leq r$, and where $H_0 = S$ and $H_r = G$. Since $H_{i-1} \triangleleft H_i$, it follows that $H_{i-1} \cap K \triangleleft H_i \cap K$, and so we have

$$S \cap K = H_0 \cap K \triangleleft H_1 \cap K \triangleleft \cdots \triangleleft H_r \cap K = G \cap K = K,$$

and thus $S \cap K \triangleleft\triangleleft K$, as required. ■

2.4. Corollary. *Let S and T be subnormal subgroups of a group G . Then $S \cap T \triangleleft\triangleleft G$.*

Proof. We have $S \cap T \triangleleft\triangleleft T$ by Lemma 2.3, and since $T \triangleleft\triangleleft G$, it follows by the transitivity of subnormality that $S \cap T \triangleleft\triangleleft G$, as asserted. ■

If S and T are normal subgroups of a group G , then, of course, their intersection $S \cap T$ is also normal, and so too is their join, $\langle S, T \rangle = ST$. In other words, the collection of normal subgroups of an arbitrary group forms a sublattice of the full subgroup lattice. It is perhaps surprising, and it is certainly less trivial, that the same conclusion holds for subnormal subgroups of finite groups. We have just seen that the collection of subnormal subgroups of G is closed under intersections, and that was easy. The deeper result is that this collection is also closed under joins if $|G|$ is finite. We should mention, however, that there are counterexamples that show that

joins of subnormal subgroups can fail to be subnormal in the general infinite case.

2.5. Theorem. *Let G be a finite group, and suppose that $S, T \triangleleft\triangleleft G$. Then $\langle S, T \rangle \triangleleft\triangleleft G$.*

There are several known proofs of this remarkable theorem of Wielandt, which was first established in 1939. Wielandt's original argument proceeded via double induction directly from the definition of subnormality, and it is also valid for some infinite groups: those which satisfy the ascending chain condition on subnormal subgroups. Our proof, on the other hand, relies on a later result of Wielandt, and it makes sense only in the finite case. But it is less technical than Wielandt's, and it seems somewhat more conceptual.

Before we prove Theorem 2.5, we need to develop some more theory, including the following pretty result (of Wielandt, of course).

2.6. Theorem. *Let $S \triangleleft\triangleleft G$, where G is a finite group, and let M be a minimal normal subgroup of G . Then $M \subseteq \mathbf{N}_G(S)$.*

Recall that a **minimal normal** subgroup of G is a nonidentity normal subgroup M of G such that the only normal subgroup of G that is properly contained in M is the identity. For example, if G is simple, then G is a minimal normal subgroup of itself.

To prove Theorem 2.6, we must digress briefly to discuss the **socle** of a finite group G , which is the subgroup generated by all minimal normal subgroups of G , and which is denoted $\text{Soc}(G)$. (Of course, the subgroup generated by a collection of normal subgroups is just the product of those subgroups.)

The key observation here is that since G is finite, every nonidentity normal subgroup N of G contains a minimal normal subgroup of G , and thus $N \cap \text{Soc}(G) > 1$. In particular, if $G > 1$, then $\text{Soc}(G) > 1$.

We remind the reader of a useful general fact, which is needed in the proof of Theorem 2.6.

2.7. Lemma. *Let M and N be normal subgroups of a group G , and assume $M \cap N = 1$. Then every element of M commutes with every element of N .*

Proof. Let $m \in M$ and $n \in N$ and consider the commutator $c = [m, n]$, which, by definition, is the element $m^{-1}n^{-1}mn$. Since $c = m^{-1}m^n$ and M is normal, we see that $c \in M$. But also, $c = (n^{-1})^m n$, and thus $c \in N$ because N is normal. Then $c \in M \cap N = 1$, and so $1 = c = m^{-1}m^n$, and we deduce that $m^n = m$. It follows that m and n commute, as asserted. ■

Proof of Theorem 2.6. We proceed by induction on $|G|$. There is nothing to prove if $S = G$, and so we can assume that $S < G$. Then since $S \triangleleft\triangleleft G$, we

can reason as we did previously to find a subgroup $N \triangleleft G$ with $S \triangleleft\triangleleft N < G$. (Simply take N to be the penultimate term of a subnormal series with distinct terms climbing from S to G .)

There are now two cases. If $M \cap N = 1$, then by Lemma 2.7, we have $M \subseteq \mathbf{C}_G(N) \subseteq \mathbf{C}_G(S) \subseteq \mathbf{N}_G(S)$, as wanted. We can suppose, therefore, that $1 < M \cap N$. Then since $M \cap N \subseteq M$, it follows from the fact that M is minimal normal in G that $M \cap N = M$, and we have $M \subseteq N$.

Since $S \triangleleft\triangleleft N < G$, the inductive hypothesis guarantees that every minimal normal subgroup of N normalizes S . Now $M \triangleleft N$, but we do not know that M is minimal normal in N , and so we cannot conclude directly that M normalizes S . But we do know that $\text{Soc}(N)$ normalizes S , and so it will suffice to show that $M \subseteq \text{Soc}(N)$.

First, observe that $M \cap \text{Soc}(N) > 1$ since $1 < M \triangleleft N$. Also, $\text{Soc}(N)$ is characteristic in N , and hence it is normal in G , and thus $M \cap \text{Soc}(N) \triangleleft G$. But $1 < M \cap \text{Soc}(N) \subseteq M$, and it follows from the fact that M is minimal normal in G that $M \cap \text{Soc}(N) = M$. Then $M \subseteq \text{Soc}(N) \subseteq \mathbf{N}_G(S)$, and the proof is complete. ■

Finally, we are ready to prove that in finite groups, joins of subnormal subgroups are subnormal.

Proof of Theorem 2.5. We prove by induction on $|G|$ that if $S, T \triangleleft\triangleleft G$, then $\langle S, T \rangle \triangleleft\triangleleft G$. Since we can certainly assume that $G > 1$, we can choose a minimal normal subgroup M of G . Let $\overline{G} = G/M$, and observe that the images \overline{S} and \overline{T} of S and T are subnormal in \overline{G} . But $|\overline{G}| < |G|$, and so the inductive hypothesis applies, and we conclude that $\langle \overline{S}, \overline{T} \rangle \triangleleft\triangleleft \overline{G}$. Since “overbar” is a homomorphism with kernel M , it follows that

$$\langle \overline{S}, \overline{T} \rangle = \overline{\langle S, T \rangle} = \overline{\langle S, T \rangle M},$$

and thus $\overline{\langle S, T \rangle M} \triangleleft\triangleleft \overline{G}$.

The correspondence theorem yields a bijection between the set of all subgroups of \overline{G} and the set of all of those subgroups of G that contain M . Furthermore, this bijection preserves normality, and hence it also preserves subnormality, and we conclude from this that $\langle S, T \rangle M \triangleleft\triangleleft G$. But M is minimal normal in G , and thus by Theorem 2.6, each of the subgroups S and T is normalized by M . It follows that M normalizes $\langle S, T \rangle$, and we see that $\langle S, T \rangle \triangleleft \langle S, T \rangle M \triangleleft\triangleleft G$, and thus $\langle S, T \rangle$ is subnormal in G , as wanted. ■

Two subgroups H and K of a group G are said to be **permutable** if $HK = KH$. (Recall that this is equivalent to HK being a subgroup.) We know that each normal subgroup of G is permutable with all subgroups,

and it is of some interest to ask if the converse is true. Is a subgroup that is permutable with all subgroups necessarily normal? The answer is “no”, but it is true (in a finite group) that such a subgroup must be subnormal. (A subgroup permutable with all subgroups in some group G is said to be **quasinormal** in G .)

Actually, a result stronger than “quasinormal implies subnormal” is true. Given $S \subseteq G$, it is enough to know that S is permutable with all of its own conjugates to deduce that S is subnormal; one need not assume that S is permutable with every subgroup.

2.8. Theorem. *Let $S \subseteq G$, where G is a finite group, and assume that $SS^x = S^xS$ for all $x \in G$. Then $S \triangleleft\triangleleft G$.*

Since it is certainly not obvious how to construct a subnormal series from S to G in the situation of Theorem 2.8, we must find some more subtle method of proof. Trying induction on $|G|$, we see that if $S \subseteq H < G$, then the hypothesis on S is automatically satisfied in H , and so $S \triangleleft\triangleleft H$ by the inductive hypothesis. To see what good that might be, imagine what the situation would be if we were trying to prove that S is *normal* in G . We would then know that every proper subgroup of G that contains S is contained in $\mathbf{N}_G(S)$, and so if S is not actually normal in G , then $\mathbf{N}_G(S)$ would be a maximal subgroup of G . In fact, it would be the unique maximal subgroup containing S .

By the following “zipper lemma” of Wielandt, a similar conclusion holds when we are trying to prove that S is subnormal, and this is the key to the proof of Theorem 2.8.

2.9. Theorem (Zipper Lemma). *Suppose that $S \subseteq G$, where G is a finite group, and assume that $S \triangleleft\triangleleft H$ for every proper subgroup H of G that contains S . If S is not subnormal in G , then there is a unique maximal subgroup of G that contains S .*

As we have seen, the analog of the zipper lemma is true (and trivial) if “normal” replaces “subnormal”, and in that situation, the unique maximal subgroup of G that contains S is the normalizer of S . But in general, there is no such thing as a subnormalizer, and so we must work harder to prove Theorem 2.9. What we mean by saying that subnormalizers do not exist is that if $S \subseteq G$, there need not be a unique subgroup maximal with the property that it contains S subnormally. For example, a Sylow 2-subgroup P of the simple group $G = PSL(2, 7)$ of order 168 is contained in two maximal subgroups of G , each of order 24. It is not hard to check that the subgroup $\mathbf{Z}(P)$, which has order 2, is subnormal in each of these maximal subgroups, but of course, $\mathbf{Z}(P)$ cannot be subnormal in G because G is simple.

Before we prove the zipper lemma, we demonstrate how it can be used by proving Theorem 2.8. We need an easy preliminary result.

2.10. Lemma. *Let $H \subseteq G$, where G is an arbitrary group, and suppose that $HH^x = G$. Then $H = G$.*

Proof. Write $x = uv$, where $u \in H$ and $v \in H^x$. Then $xv^{-1} = u$ and we have

$$H^x = (H^x)^{v^{-1}} = H^u = H,$$

where the first equality holds because $v \in H^x$ and the third holds because $u \in H$. Then $G = HH^x = HH = H$ and the proof is complete. ■

We also need a bit of notation. If H is an arbitrary subgroup of G , we write $H^G = \langle H^x \mid x \in G \rangle$. This is the **normal closure** of H in G , and we see that $H^G \triangleleft G$ because conjugation by elements of G simply permutes the generating subgroups of H^G . In fact, H^G is the unique smallest normal subgroup of G containing H since if $H \subseteq N \triangleleft G$, then N contains all conjugates of H , and thus N contains the subgroup H^G generated by these conjugates.

Proof of Theorem 2.8. Working by induction on $|G|$, we can assume that S is subnormal in every subgroup H such that $S \subseteq H < G$. Assuming that S is not subnormal in G , we have $S < G$, and we derive a contradiction.

By the zipper lemma, S is contained in a unique maximal subgroup M of G . Now consider a conjugate S^x of S . Since $S < G$, Lemma 2.10 guarantees that $SS^x < G$, and since SS^x is a subgroup because $SS^x = S^xS$ by hypothesis, we conclude that SS^x is contained in some maximal subgroup of G . But the only maximal subgroup containing S is M , and so we must have $SS^x \subseteq M$. Then $S^x \subseteq M$ for all elements $x \in G$.

Now consider the normal closure $S^G = \langle S^x \mid x \in G \rangle$. By the result of the previous paragraph, we know that $S^G \subseteq M$, and thus $S^G < G$. It follows that $S \triangleleft\triangleleft S^G \triangleleft G$, and thus $S \triangleleft\triangleleft G$. This is a contradiction, and the proof is complete. ■

We now prove the Wielandt zipper lemma.

Proof of Theorem 2.9. Work by induction on $|G : S|$. Since we are assuming that S is not subnormal in G , we certainly have $S < G$, and thus the case $|G : S| = 1$ of the theorem is vacuously satisfied and our induction starts.

As S is not normal, we have $N_G(S) < G$, and thus $N_G(S) \subseteq M$ for some maximal subgroup M of G . Of course $S \subseteq M$, and our task is to show

that M is the only maximal subgroup of G that contains S . Suppose then, that also $S \subseteq K$, where K is maximal in G . We work to show that $K = M$.

Now $S \subseteq K < G$, and so by hypothesis, $S \triangleleft\triangleleft K$. Suppose that in fact $S \triangleleft K$. Then $K \subseteq \mathbf{N}_G(S) \subseteq M$, and since K is maximal in G , it follows that $K = M$, as wanted. We can suppose, therefore, that S is not normal in K .

Since $S \triangleleft\triangleleft K$, there is some shortest subnormal series

$$S = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = K,$$

and we see that $r \geq 2$. Also, S is not normal in H_2 since otherwise we could delete H_1 to obtain a shorter subnormal series for S in K . Let $x \in H_2$ with $S^x \neq S$ and write $T = \langle S, S^x \rangle$. Note that $T \subseteq K$ since $S \subseteq K$ and $x \in K$. Also, $S^x \subseteq (H_1)^x = H_1 \subseteq \mathbf{N}_G(S)$, and thus $T \subseteq \mathbf{N}_G(S) \subseteq M$. Furthermore, we see that $S \triangleleft T < G$.

Observe that S^x satisfies the hypotheses imposed on S in the statement of the theorem. (This, of course, is because conjugation by x defines an automorphism of G .) We claim that the subgroup $T = \langle S, S^x \rangle$ also satisfies these hypotheses. Specifically, we need to show that if $T \subseteq H < G$, then $T \triangleleft\triangleleft H$ and that T is not subnormal in G .

First, if $T \subseteq H < G$, then clearly $S \subseteq H$, and thus $S \triangleleft\triangleleft H$, and similarly, $S^x \triangleleft\triangleleft H$. Then T is the join of two subnormal subgroups of H , and we conclude by Theorem 2.5 that $T \triangleleft\triangleleft H$ as wanted. Also, $S \triangleleft T$, and so if $T \triangleleft\triangleleft G$, it would follow that $S \triangleleft\triangleleft G$, which is not the case. Thus T is not subnormal, as claimed.

Now $T > S$ since S^x is contained in T , but it is not contained in S . Then $|G : T| < |G : S|$, and so by the inductive hypothesis, T is contained in a unique maximal subgroup of G . On the other hand, we know that $T \subseteq M$ and $T \subseteq K$, and thus $M = K$. The proof is now complete. ■

Perhaps we should explain the name “zipper lemma”. The key idea of the proof of Theorem 2.9 is that if S is contained in two different maximal subgroups, then some larger subgroup T is also contained in two different maximal subgroups. Repeating this argument, we would get a still larger subgroup contained in two different maximal subgroups, and so on. But this cannot go on indefinitely in a finite group. As we climb higher, the two maximal subgroups are forced to be the same. This is analogous to zipping up an open zipper. As we pull up on the zipper pull, the two top parts of the zipper are forced together.

We conclude this section with another application of the zipper lemma.

2.11. Theorem. *Let A be an abelian subgroup of a finite group G , and assume that for every subgroup H with $A \subseteq H \subseteq G$, we have $|H : A|^2 \leq |H : \mathbf{Z}(H)|$. Then $A \subseteq \mathbf{F}(G)$.*

The condition that $|H : A|^2 \leq |H : \mathbf{Z}(H)|$ for all subgroups H such that $A \subseteq H \subseteq G$ may seem somewhat artificial, but in fact, it arises naturally in character theory. If A is abelian and some character of A induces irreducibly to G , then this condition is automatically satisfied. Also, we observe that if A is abelian and satisfies this condition, then $A = \mathbf{C}_G(A)$. To see this, take $H = \mathbf{C}_G(A)$ and note that $|H : \mathbf{Z}(H)| \leq |H : A|$, and so the assumed inequality forces $|H : A| = 1$.

Proof of Theorem 2.11. Working by induction on $|G|$, we can assume that $A \subseteq \mathbf{F}(H)$ whenever $A \subseteq H < G$, and thus $A \triangleleft\triangleleft H$. Also, by Theorem 2.2, we are done if $A \triangleleft\triangleleft G$, and so we can assume that A is not subnormal in G , and the zipper lemma applies. We conclude, therefore, that there is a unique maximal subgroup M containing A .

Now let $g \in G$. If $\langle A, A^g \rangle < G$, then $\langle A, A^g \rangle$ is contained in some maximal subgroup of G , and hence $\langle A, A^g \rangle \subseteq M$, and in particular, $A^g \subseteq M$. If this happens for all $g \in G$, then $A^G \subseteq M$, and thus $A^G < G$ and we have $A \triangleleft\triangleleft A^G \triangleleft G$, which is a contradiction. We conclude that $G = \langle A, A^g \rangle$ for some element $g \in G$.

Since A and A^g are abelian, we have $A \cap A^g \subseteq \mathbf{Z}(G)$, and it follows that

$$|G| > |AA^g| = \frac{|A|^2}{|A \cap A^g|} \geq \frac{|A|^2}{|\mathbf{Z}(G)|},$$

where the strict inequality follows by Lemma 2.10 since $A < G$. Multiplying both sides by $|G|/|A|^2$, we conclude that $|G : A|^2 > |G : \mathbf{Z}(G)|$, contrary to the hypothesis. ■

Problems 2A

2A.1. Let π be a set of prime numbers, and recall that $\mathbf{O}_\pi(G)$ is the unique largest normal π -subgroup of G . Show that $\mathbf{O}_\pi(G)$ contains every subnormal π -subgroup of G . Conclude that the subgroup generated by two subnormal π -subgroups of G is itself a π -subgroup.

2A.2. Again let π be a set of prime numbers, and recall that $\mathbf{O}^\pi(G)$ is the unique smallest normal subgroup of G whose factor group is a π -group. If $K \triangleleft\triangleleft G$ and $|G : K|$ is a π -number, show that $K \supseteq \mathbf{O}^\pi(G)$.

2A.3. Let $H, K \subseteq G$ and suppose that $|G : H|$ and $|K|$ are relatively prime.

(a) If $H \triangleleft\triangleleft G$, show $K \subseteq H$.

(b) If $K \triangleleft\triangleleft G$, show $K \subseteq H$.

2A.4. Let $S \subseteq G$, where G is a finite group and S is simple, and suppose that $SH = HS$ for all subnormal subgroups H of G . Show that $S \subseteq \mathbf{N}_G(H)$ for all $H \triangleleft\triangleleft G$.

Note. The intersection of the normalizers of all subnormal subgroups of a group G is the **Wielandt subgroup** of G .

2A.5. Let \mathcal{X} be any collection of minimal normal subgroups of G , and let $N = \prod \mathcal{X}$.

(a) Show that N is the direct product of some of the members of \mathcal{X} .

(b) Show that every minimal normal subgroup of N is simple.

(c) Show that N is a direct product of simple groups.

Hint. For (b), show that $\text{Soc}(N) = N$.

Note. This problem shows that minimal normal subgroups and socles of finite groups are direct products of simple groups.

2A.6. In this situation of the previous problem, show that every nonabelian normal subgroup of G contained in N contains a member of \mathcal{X} .

2A.7. Let $S \triangleleft\triangleleft G$, where S is nonabelian and simple. Show that S^G is a minimal normal subgroup of G .

Hint. Work by induction on $|G|$ to conclude that $S \subseteq \text{Soc}(H)$ whenever $S \subseteq H$. Deduce that each conjugate of S in G is a minimal normal subgroup of S^G . Then apply the previous problem to the group S^G , where \mathcal{X} is the set of all G -conjugates of S .

2A.8. Let S and T be different nonabelian subnormal simple subgroups of G . Show that S and T commute elementwise.

2A.9. Let $H \triangleleft\triangleleft G$ and assume that $H = \mathbf{O}^\pi(H)$, where π is a set of primes. Show that $\mathbf{O}_\pi(G)$ normalizes H .

Hint. It is no loss to assume that $G = H\mathbf{O}_\pi(G)$. Show in this case that $H = \mathbf{O}^\pi(H)$.

2A.10. We say that subgroups $H, K \subseteq G$ are **strongly conjugate** if they are conjugate in the group $\langle H, K \rangle$. Show that $H \triangleleft\triangleleft G$ if and only if the only subgroup of G that is strongly conjugate to H is H itself.

2B

In this section, we present a useful result that is essentially due to R. Baer, and which we derive from the Wielandt zipper lemma. Versions of Baer's theorem have also been proved by M. Suzuki and by J. Alperin and R. Lyons.

2.12. Theorem (Baer). *Let H be a subgroup of a finite group G . Then $H \subseteq \mathbf{F}(G)$ if and only if $\langle H, H^x \rangle$ is nilpotent for all $x \in G$.*

Proof. One direction is trivial. If $H \subseteq \mathbf{F}(G)$, then also $H^x \subseteq \mathbf{F}(G)$ since $\mathbf{F}(G) \triangleleft G$. Then $\langle H, H^x \rangle$ is a subgroup of the nilpotent group $\mathbf{F}(G)$, and hence it is nilpotent.

Conversely, assume that $\langle H, H^x \rangle$ is nilpotent for all $x \in G$. In particular, H is nilpotent, and so to prove that $H \subseteq \mathbf{F}(G)$, it suffices by Theorem 2.2 to prove that $H \triangleleft\triangleleft G$. We establish this by induction on $|G|$. Assume that H is not subnormal in G , and observe that if H is contained in a proper subgroup K , then $\langle H, H^x \rangle$ is nilpotent for all $x \in K$, and thus $H \triangleleft\triangleleft K$ by the inductive hypothesis. The zipper lemma now applies, and we deduce that H is contained in a unique maximal subgroup M .

Now consider a conjugate H^x of H . If $\langle H, H^x \rangle = G$, then G is nilpotent, and hence $H \triangleleft\triangleleft G$, which is not the case. Then $\langle H, H^x \rangle < G$, and so this subgroup must be contained in some maximal subgroup of G . But $\langle H, H^x \rangle$ contains H , and the only maximal subgroup of G that contains H is M . It follows that $\langle H, H^x \rangle \subseteq M$, and we conclude that M contains all conjugates of H in G , and so $H^G \subseteq M$. The normal closure H^G is thus proper in G , and we have $H \subseteq H^G < G$. Then, $H \triangleleft\triangleleft H^G \triangleleft G$, and so $H \triangleleft\triangleleft G$. This contradiction shows that $H \triangleleft\triangleleft G$, as required. ■

The following is a useful consequence of Baer's theorem. Theorem 2.13 is the key to Matsuyama's extension to groups of even order of Goldschmidt's non-character proof of the Burnside $p^a q^b$ -theorem. (Goldschmidt required that both primes were odd, and Matsuyama removed that restriction.)

Recall that an **involution** in a group G is any element of order 2.

2.13. Theorem. *Let t be an involution in a finite group G , and assume that $t \notin \mathbf{O}_2(G)$. Then there exists an element $x \in G$ of odd prime order such that $x^t = x^{-1}$.*

Since $\mathbf{O}_2(G)$ is the unique largest normal 2-subgroup of G , the condition that $t \notin \mathbf{O}_2(G)$ says that t is not contained in any normal 2-subgroup of G .

In order to prove Theorem 2.13, we need to digress briefly. A group D is **dihedral** if it contains a nontrivial cyclic subgroup C of index 2 such that every element of $D - C$ is an involution. Of course, $|D| = 2|C|$, and so dihedral groups have even order at least 4, and it is not hard to show

that a dihedral group is determined up to isomorphism by its order. Group theorists usually refer to the dihedral group of order $2n$ as D_{2n} , and that is the notation we use here. (But this notation is not completely standard, and this group is often referred to as D_n .) The dihedral group D_4 is isomorphic to the Klein group $C_2 \times C_2$, and except for this degenerate case, dihedral groups are always nonabelian. It is easy to see that D_{2n} exists for $n > 2$: it is the group of rotational symmetries in 3-space of a regular n -gon. (In Chapter 3, we shall see how to construct dihedral groups as semidirect products, thereby establishing their existence without relying on geometric reasoning.)

The following presents some of the basic facts about dihedral groups.

2.14. Lemma. *Let D be a group.*

- (a) *Suppose that $C = \langle c \rangle$ is a nontrivial cyclic subgroup of index 2 in D , and that $t \in D - C$ is an involution. Then every element of $D - C$ is an involution if and only if $c^t = c^{-1}$. In this case, D is dihedral, and $x^y = x^{-1}$ for all $x \in C$ and $y \in D - C$. Also, D is generated by the distinct involutions ct and t .*
- (b) *Suppose that D is generated by distinct involutions s and t . Then the cyclic subgroup $C = \langle st \rangle$ is nontrivial, and it fails to contain s and t . Also $|D : C| = 2$, and t inverts the generator st of C . In particular, we are in the above situation, and D is dihedral.*

Proof. For (a), observe that $D - C$ is exactly the coset Ct . If $a \in C$ then $(at)^2 = atat = aa^t$, and thus $a^t = a^{-1}$ if and only if $(at)^2 = 1$. In particular, if every element of $D - C$ is an involution, then $(ct)^2 = 1$, and so $c^t = c^{-1}$. Conversely, suppose that $c^t = c^{-1}$. Since every element of C is a power of c , we have $a^t = a^{-1}$ for all $a \in C$, and hence $(at)^2 = 1$, and every element of $D - C = Ct$ is an involution. In other words, D is dihedral. Let $x \in C$ and $y \in D - C$. Then $y = at$ for some element $a \in C$, and we have $x^y = x^{at} = x^t = x^{-1}$. Also, ct is an involution, and the group $\langle ct, t \rangle$ properly contains $C = \langle c \rangle$, and thus it is the whole group D . Finally, ct and t are distinct because $c \neq 1$.

Now assume the situation of (b) and observe that C is nontrivial since $s \neq t$. We have $(st)^t = t(st)t = ts = (st)^{-1}$, and thus t inverts the generator st of C , as wanted. Then $C^t = \langle st \rangle^t = \langle (st)^t \rangle = \langle (st)^{-1} \rangle = C$, and so $t \in \mathbf{N}_D(C)$. It follows that $C\langle t \rangle$ is a subgroup containing both t and $(st)t = s$, and thus $C\langle t \rangle$ is all of D . Because $st \in C$, we see that if either s or t lies in C , then both s and t lie in C , and this is impossible since a cyclic group can contain at most one involution. Thus C contains neither s or t , and in particular, $C \cap \langle t \rangle = 1$. Since $D = C\langle t \rangle$, we have $|D : C| = |\langle t \rangle| = 2$, and this completes the proof of (b). ■

The fact that two elements of order 2 in an arbitrary group always generate a dihedral subgroup does not seem to generalize. There appears to be almost nothing that can be said about the structure of a subgroup generated by two elements of given orders $m > 1$ and $n > 1$ in any case other than $m = 2 = n$.

Proof of Theorem 2.13. Let $T = \langle t \rangle$. If $T \subseteq \mathbf{F}(G)$, then T is contained in the unique Sylow 2-subgroup of $\mathbf{F}(G)$, which is $\mathbf{O}_2(G)$, contrary to hypothesis. By Baer's theorem (2.12) therefore, there exists $g \in G$ such that $\langle T^g, T \rangle$ is not nilpotent. In particular, $\langle t^g, t \rangle$ is not a 2-group.

By Lemma 2.14, it follows that $D = \langle t^g, t \rangle$ is dihedral of order $2|C|$, where C is a cyclic subgroup whose elements are inverted by t . Since D is not a 2-group, neither is G , and thus there exists an element $x \in C$ of odd prime order. Since $x^t = x^{-1}$, the proof is complete. ■

Problems 2B

2B.1. Let $H \subseteq G$ and assume that for each element $g \in G$, either $\langle H, H^g \rangle$ is nilpotent or $HH^g = H^gH$. Show that $H \triangleleft\triangleleft G$.

2B.2. Let D be the dihedral group of order $2n$.

- (a) If n is odd, show that D contains exactly n involutions, and that they all lie in a single conjugacy class.
- (b) If n is even, show that D contains exactly $n + 1$ involutions, and these lie in exactly three conjugacy classes, with sizes 1, $n/2$ and $n/2$, respectively.

2B.3. Let s and t be involutions in a group G . If s and t are not conjugate in G , show that there exists an involution $z \in G$, different from s and t , and commuting with both of them.

2B.4. Suppose that G has more than one Sylow 2-subgroup and that every two distinct Sylow 2-subgroups of G intersect trivially. Show that G contains exactly one conjugacy class of involutions.

2B.5. Let $B \subseteq G$, with $|G : B| = 2$. Show that the following are equivalent.

- (1) $G - B$ contains an involution t such that $b^t = b^{-1}$ for all elements $b \in B$.
- (2) $G - B$ consists entirely of involutions.
- (3) Every element t of $G - B$ is an involution such that $b^t = b^{-1}$ for all elements $b \in B$.

Show also that if these conditions hold, then B must be abelian.

Note. In this situation, G is said to be **generalized dihedral**.

2B.6. Show that G has a normal Sylow p -subgroup if and only if every subgroup of the form $\langle x, y \rangle$ has a normal Sylow p -subgroup, where x and y are conjugate elements of G having p -power order.

2C

Although there really is no connection with subnormality, we digress in this section to discuss the terms “local” and “global” as they are used in finite group theory. (And then we will present an application of Theorem 2.13 in this context.) By definition, a subgroup H of a group G is **p -local**, where p is prime, if H is of the form $H = \mathbf{N}_G(P)$, where P is some nonidentity p -subgroup of G . More generally, a subgroup is **local** if it is p -local for some prime p . The idea here is that in some sense, the local subgroups are those that are easiest to find: choose a Sylow subgroup, pick a nontrivial subgroup of it, and then take the normalizer.

For example, suppose we want to prove that up to isomorphism, the only simple group of order 60 is the alternating group A_5 . To establish this, it suffices to show that an arbitrary simple group G of order 60 must have a subgroup H of index 5. Then the action of G on the set of right cosets of H yields an isomorphism from G into A_5 , and because $|G| = 60$, this map must be surjective, and $G \cong A_5$, as required.

Given a simple group G of order 60, we can find the required subgroup H , as follows. The number n_2 of Sylow 2-subgroups of G must be either 5 or 15. If $n_2 = 5$, take H to be the normalizer of a Sylow 2-subgroup of G . If $n_2 = 15$, then since $15 - 1$ is not divisible by 4, it follows by Theorem 1.16 that there exist distinct Sylow 2-subgroups S and T that intersect nontrivially. Let $D = S \cap T > 1$ and $H = \mathbf{N}_G(D)$. Then H contains both S and T , and thus $|H|$ is a proper multiple of 4. Since G is simple, D is not normal, and so $H < G$. Also, $|G : H| \neq 3$ by the $n!$ -theorem, and the only remaining possibility is that H has index 5, as wanted.

In both cases, where $n_2 = 5$ and where $n_2 = 15$, we found a 2-local subgroup of index 5, and as we explained, this shows that $G \cong A_5$. (Actually, since $n_2(A_5) = 5$, we see that the case $n_2 = 15$ does not occur, but nevertheless, it had to be considered.)

Now consider the analogous problem for A_6 . It is true that every simple group of order 360 is isomorphic to A_6 , but this is considerably more difficult to prove. It would suffice to find a subgroup of index 6 in an arbitrary simple group of order 360, but this is hard to do because no *local* subgroup of A_6 has index 6, and so no argument such as we used for A_5 can possibly work. In fact, all subgroups of index 6 in A_6 are isomorphic to A_5 , and hence

they are simple. No subgroup of index 6, therefore, can be the normalizer of anything in a simple group of order 360. Although it is possible, using character theory, to show that a simple group of order 360 really does have a subgroup of index 6, the usual proof that up to isomorphism, there is a unique simple group of order 360 proceeds by showing that every such group is isomorphic to $PSL(2, 9)$. (Of course, it follows that A_6 and $PSL(2, 9)$ are isomorphic.)

Properties of groups that do not directly refer to local subgroups are often referred to as **global** properties. What is remarkable, is how often it happens that global information can be deduced from appropriate data about local subgroups. For example, here is a “local-to-global” result that is not terribly difficult to prove.

2.15. Theorem. *Suppose that for every odd prime p , every p -local subgroup of a finite group G has a normal Sylow 2-subgroup. Then G has a normal Sylow 2-subgroup.*

If a group G has a normal Sylow 2-subgroup, it is easy to see that every subgroup of G also has a normal Sylow 2-subgroup. Theorem 2.15 can thus be viewed as a strong converse to this remark. Its proof relies on Theorem 2.13 together with the general observation that local subgroups of homomorphic images are images of local subgroups. (We state this a bit more precisely, as follows.)

2.16. Lemma. *Let $N \triangleleft G$, and write $\overline{G} = G/N$, using the standard “bar convention”, where overbar is the canonical homomorphism $G \rightarrow \overline{G}$. Then for all primes p , every p -local subgroup of \overline{G} has the form \overline{L} , where L is some p -local subgroup of G .*

Proof. By the correspondence theorem, every subgroup of \overline{G} has the form \overline{H} , for some subgroup H of G with $H \supseteq N$. Now let $N \subseteq M \subseteq G$, where \overline{M} is p -local in \overline{G} . Although M may not be p -local in G , we will complete the proof by showing that $\overline{M} = \overline{L}$ for some p -local subgroup L of G .

Since \overline{M} is p -local, it is the normalizer in \overline{G} of some nontrivial p -subgroup, which we can write in the form \overline{U} , where $N < U \subseteq G$ and $|U : N|$ is a power of p . Then $\overline{M} = \mathbf{N}_{\overline{G}}(\overline{U})$, and since $U \supseteq N$, it follows that $M = \mathbf{N}_G(U)$.

Let $P \in \text{Syl}_p(U)$, and let $L = \mathbf{N}_G(P)$. Now $U = NP$ because N and P have coprime indices in U , and since $N < U$, it follows that $P > 1$, and thus L is p -local in G . Since L normalizes both N and P , we have $L \subseteq \mathbf{N}_G(NP) = \mathbf{N}_G(U) = M$, and thus $\overline{L} \subseteq \overline{M}$. To obtain the reverse containment, observe that since $U \triangleleft M$ and $P \in \text{Syl}_p(U)$, the Frattini argument yields

$$M = U\mathbf{N}_M(P) = NP\mathbf{N}_M(P) = N\mathbf{N}_M(P) \subseteq NL.$$

Then $\overline{M} \subseteq \overline{NL} = \overline{L}$, where the equality holds because N is the kernel of the overbar homomorphism. It follows that $\overline{M} = \overline{L}$, as wanted. ■

Proof of Theorem 2.15. First, we suppose that $\mathbf{O}_2(G) = 1$, and we show in this case that $|G|$ is odd. If G has even order, we can choose an involution $t \in G$, and we observe that $t \notin \mathbf{O}_2(G)$. Then by Theorem 2.13, there exists an element x of odd prime order p such that $x^t = x^{-1}$. Let $X = \langle x \rangle$, and note that $t \in \mathbf{N}_G(X)$ and that $\mathbf{N}_G(X)$ is p -local. By hypothesis, $\mathbf{N}_G(X)$ has a normal Sylow 2-subgroup S , which necessarily contains t . As X and S are normal in $\mathbf{N}_G(X)$ and $X \cap S = 1$, it follows by Lemma 2.7 that X and S centralize each other, and in particular, t centralizes x . Thus $x = x^t = x^{-1}$, and this is a contradiction since x has order $p > 2$. This shows that $|G|$ is odd, as wanted.

In the general case, let $N = \mathbf{O}_2(G)$, and observe that by the previous lemma, the p -local subgroups of $\overline{G} = G/N$ are homomorphic images of p -local subgroups of G for all odd primes p . By hypothesis, the p -local subgroups of G have normal Sylow 2-subgroups, and thus the same is true for their homomorphic images, and it follows that \overline{G} satisfies the hypotheses of the theorem. But $\mathbf{O}_2(\overline{G})$ is trivial, and by the first part of the proof it follows that $|\overline{G}|$ is odd. Then $N = \mathbf{O}_2(G)$ is a normal Sylow 2-subgroup of G , and the proof is complete. ■

We close this section with a lemma that will be needed later. Although this result has nothing to do with subnormality, it is related to Lemma 2.16, and so it seems appropriate to present it here. The assertion of Lemma 2.16 is that every p -local subgroup of a homomorphic image of G is the image of a p -local subgroup of G . This suggests the question of whether or not the image of a p -local subgroup must be p -local. The answer is “not always”. For example, if $\mathbf{O}_p(G)$ is nontrivial, then G is p -local in itself, but this cannot be true for $G/\mathbf{O}_p(G)$, which has no nonidentity normal p -subgroup. But p -local subgroups do map to p -local subgroups if the kernel of the homomorphism is a p' -group.

2.17. Lemma. *Let G be a finite group, and let $N \triangleleft G$. Write $\overline{G} = G/N$, and let p be a prime that does not divide $|N|$. If P is a nontrivial p -subgroup of G , then \overline{P} is nontrivial, and $\mathbf{N}_{\overline{G}}(\overline{P}) = \overline{\mathbf{N}_G(P)}$. In particular, if L is p -local in G , then \overline{L} is p -local in \overline{G} .*

Proof. Since the p -group P is nontrivial, and the order of N is not divisible by p , we have $P \not\subseteq N$, and thus \overline{P} is nontrivial. Write $L = \mathbf{N}_G(P)$, and observe that $\overline{P} \triangleleft \overline{L}$ because overbar is a homomorphism. Thus $\overline{L} \subseteq \mathbf{N}_{\overline{G}}(\overline{P})$ and it suffices to prove the reverse containment.

By the correspondence theorem, every subgroup of \overline{G} has the form \overline{X} for some (unique) subgroup $X \subseteq G$ with $X \supseteq N$, and so in particular, we can write $\mathbf{N}_{\overline{G}}(\overline{P}) = \overline{M}$, where $N \subseteq M \subseteq G$. Now $\overline{PN} = \overline{P} \triangleleft \overline{M}$, and thus $PN \triangleleft M$ by the correspondence theorem. Also, $P \in \text{Syl}_p(PN)$ since p does not divide $|N|$, and thus by the Frattini argument, we have $M = \mathbf{N}_M(P)(PN) = \mathbf{N}_M(P)N \subseteq \mathbf{N}_G(P)N = LN$. This yields $\mathbf{N}_{\overline{G}}(\overline{P}) = \overline{M} \subseteq \overline{L}$, as wanted. The last statement should now be clear. ■

Problems 2C

2C.1. A finite group G is said to be an **N-group** if every local subgroup is solvable.

- (a) Show that every proper homomorphic image of an N-group is solvable.
- (b) Let G be a nonsolvable N-group. Show that G has a unique minimal normal subgroup S , and that S is nonabelian simple.

Hint. The Frattini argument is relevant. Also, recall that subgroups and homomorphic images of solvable groups are solvable and that if $K \triangleleft L$ with K and L/K both solvable, then L is solvable.

Note. A major step leading toward the classification of finite simple groups was J. Thompson's classification of nonsolvable N-groups. A nonabelian finite simple group is **minimal simple** if every proper subgroup is solvable, and since minimal simple groups are clearly N-groups, Thompson's work provided a classification of all minimal simple groups.

2D

Next, we present an amazing result of Zenkov. It is another application of Baer's theorem.

2.18. Theorem (Zenkov). *Let A and B be abelian subgroups of a finite group G , and let M be a minimal member of the set $\{A \cap B^g \mid g \in G\}$. Then $M \subseteq \mathbf{F}(G)$.*

The assumption in Theorem 2.18 that M is a “minimal member” of some set of subgroups means, as usual, that no member of the set is properly contained in M . Of course, if M is chosen to have minimal order among members of the set, then M will necessarily be minimal in this sense, but not conversely since in general, a minimal member of some collection of subgroups need not have minimal order.

Suppose that G has an abelian Sylow p -subgroup P . If we apply Zenkov's theorem with $A = P = B$, we deduce that $P \cap P^g \subseteq \mathbf{F}(G)$ for some element $g \in G$, and thus $P \cap P^g \subseteq \mathbf{O}_p(G)$, which is the unique Sylow p -subgroup of $\mathbf{F}(G)$. We know, however, that in general, $\mathbf{O}_p(G)$ is contained in every Sylow p -subgroup of G , and it follows in this case that $P \cap P^g = \mathbf{O}_p(G)$. In other words, if G has abelian Sylow p -subgroups, then $\mathbf{O}_p(G)$ is the intersection of two of them. This is exactly Brodkey's theorem, which appeared in the previous chapter as Theorem 1.37. We can view Zenkov's theorem, therefore, as a far-reaching generalization of Brodkey's result.

Proof of Theorem 2.18. The set $\{A \cap B^g \mid g \in G\}$ is unchanged if we replace B by an arbitrary G -conjugate B^g , and thus it is no loss to assume that $M = A \cap B$. We show by induction on $|G|$ that $M \subseteq \mathbf{F}(G)$. First, suppose that $G = \langle A, B^g \rangle$ for some element $g \in G$. Since A and B^g are abelian, we have $A \cap B^g \subseteq \mathbf{Z}(G)$, and thus $A \cap B^g = (A \cap B^g)^{g^{-1}} \subseteq B$. It follows that $A \cap B^g \subseteq A \cap B = M$, and by the minimality of M we have $M = A \cap B^g \subseteq \mathbf{Z}(G) \subseteq \mathbf{F}(G)$, as required.

We can now assume that $\langle A, B^g \rangle < G$ for all $g \in G$. To show that $M \subseteq \mathbf{F}(G)$, it is enough to prove for all primes p that a full Sylow p -subgroup P of M is contained in $\mathbf{F}(G)$. (This suffices, of course, because M is generated by its Sylow subgroups.) By Baer's theorem (2.12), therefore, it is enough to show that $\langle P, P^g \rangle$ is nilpotent for all elements $g \in G$.

Fix $g \in G$ and let $H = \langle A, B^g \rangle$, so that $H < G$. Write $C = B \cap H$, and observe that if $h \in H$, then $A \cap G^h = A \cap (B \cap H)^h = A \cap B^h \cap H = A \cap B^h$, where the final equality holds because $A \subseteq H$. In particular, $M = A \cap B = A \cap G$ is minimal in the set $\{A \cap C^h \mid h \in H\}$. By the inductive hypothesis applied in H , and with C replacing B , we conclude that $P \subseteq M \subseteq \mathbf{F}(H)$, and thus $P \subseteq \mathbf{O}_p(H)$ since $\mathbf{O}_p(H)$ is the unique Sylow p -subgroup of $\mathbf{F}(H)$. Also, $P^g \subseteq B^g \subseteq H$, and thus P^g normalizes $\mathbf{O}_p(H)$ and $\mathbf{O}_p(H)P^g$ is a p -group containing $\langle P, P^g \rangle$. In particular, $\langle P, P^g \rangle$ is a p -group, and hence it is nilpotent, as required. ■

2.19. Corollary. *Let $A \subseteq G$, where A is abelian and G is a nontrivial finite group, and assume that $|A| \geq |G : A|$. Then $A \cap \mathbf{F}(G) > 1$.*

Proof. If $g \in G$, we compute that $|A||A^g| = |A|^2 \geq |A||G : A| = |G|$. Also, we can assume that $A < G$, and thus $AA^g < G$ by Lemma 2.10. This yields

$$|G| > |AA^g| = \frac{|A||A^g|}{|A \cap A^g|} \geq \frac{|G|}{|A \cap A^g|}$$

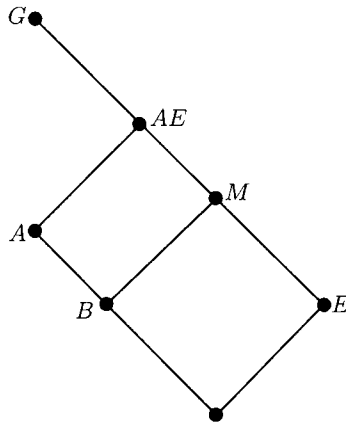
and thus $A \cap A^g > 1$. Since this holds for all $g \in G$, we can apply Zenkov's theorem with $B = A$ to deduce that $A \cap \mathbf{F}(G) > 1$, as wanted. ■

By Corollary 2.19, we see that if G is nontrivial and A is an abelian subgroup of G with $|A| \geq |G : A|$, then A contains a nontrivial subnormal subgroup of G . In fact, if A is cyclic, we get more: A contains a nontrivial *normal* subgroup of G . This is a pretty result of A. Lucchini. (We use Lucchini's theorem in Chapter 3 to prove that every automorphism of a finite group G has order less than $|G|$.)

2.20. Theorem (Lucchini). *Let A be a cyclic proper subgroup of a finite group G , and let $K = \text{core}_G(A)$. Then $|A : K| < |G : A|$, and in particular, if $|A| \geq |G : A|$, then $K > 1$.*

Proof. We proceed by induction on $|G|$. Now A/K is a proper cyclic subgroup of G/K , and the core of A/K in G/K is trivial. If $K > 1$, we can apply the inductive hypothesis in the group G/K to deduce that $|A/K| < |(G/K) : (A/K)| = |G : A|$, and there is nothing further to prove. We can assume, therefore, that $K = 1$, and we work to show that $|A| < |G : A|$.

Assume that $|A| \geq |G : A|$. Since $G > A$, we know that G is nontrivial, and hence $A \cap \mathbf{F}(G) > 1$ by Corollary 2.19. In particular, $\mathbf{F}(G) > 1$, so we can choose a minimal normal subgroup E of G with $E \subseteq \mathbf{F}(G)$. Then $E \cap \mathbf{Z}(\mathbf{F}(G)) > 1$, and since E is minimal normal in G , we have $E \subseteq \mathbf{Z}(\mathbf{F}(G))$, and in particular, E is abelian. Also, and again using the minimality of E , it follows that E is an elementary abelian p -group for some prime p . (In other words, $x^p = 1$ for all $x \in E$.)



Since $E \subseteq \mathbf{Z}(\mathbf{F}(G))$, we see that E normalizes the nontrivial group $A \cap \mathbf{F}(G)$, and of course A normalizes this subgroup too. Then $A \cap \mathbf{F}(G) \triangleleft AE$,

and since $\text{core}_G(A) = 1$, it follows that $AE < G$, as is indicated in the diagram.

Write $\overline{G} = G/E$. Let $\overline{M} = \text{core}_{\overline{G}}(\overline{A})$, with $M \supseteq E$, and note that $M \triangleleft G$ and $AM = AE$. Also, $\overline{A} < \overline{G}$ since $AE < G$, and so by the inductive hypothesis, $|\overline{A} : \overline{M}| < |\overline{G} : \overline{A}|$, and we have $|AE : M| < |G : AE|$.

Let $B = A \cap M$, so that B is cyclic. We have

$$|AE : A| = |AM : A| = |M : A \cap M| = |M : B|,$$

and hence $|AE : M| = |A : B|$. We conclude that

$$|M : B| = |AE : A| = \frac{|G : A|}{|G : AE|} < \frac{|G : A|}{|AE : M|} = \frac{|G : A|}{|A : B|} \leq \frac{|A|}{|A : B|} = |B|.$$

Suppose that M is abelian, and let $\varphi : M \rightarrow M$ be the homomorphism defined by $\varphi(m) = m^p$. Then $E \subseteq \ker(\varphi)$, and since $M = EB$ by Dedekind's lemma, it follows that $\varphi(M) = \varphi(B) \subseteq B \subseteq A$. Now $M \triangleleft G$, and hence $\varphi(M) \triangleleft G$, and we conclude that $\varphi(M) = 1$ since $\text{core}_G(A) = 1$. Then $\varphi(B) = 1$, and since B is cyclic, it follows that $|B| \leq p$. Then $|M : B| < |B| \leq p$, and since M/B is a p -group, we deduce that $M = B$. But $M \triangleleft G$ and $M \subseteq A$, and thus $M = 1$, and in particular, $E = 1$, which is a contradiction.

It follows that M is nonabelian, and since M/E is cyclic, we conclude that E is not central in M , and so $E \cap \mathbf{Z}(M) < E$. We conclude by the minimality of E that $E \cap \mathbf{Z}(M) = 1$, and thus $\mathbf{Z}(M)$ is cyclic. Since B is an abelian subgroup of M and $|M : B| < |B|$, it follows by Corollary 2.19 that $B \cap \mathbf{F}(M) > 1$. Now $\mathbf{F}(M) \subseteq \mathbf{F}(G)$, and so E centralizes $\mathbf{F}(M)$, and thus $B \cap \mathbf{F}(M)$ is a nontrivial central subgroup of $BE = M$. Since $\mathbf{Z}(M)$ is cyclic, we see that $B \cap \mathbf{F}(M)$ is characteristic in $\mathbf{Z}(M) \triangleleft G$. Thus $B \cap \mathbf{F}(M)$ is a nontrivial normal subgroup of G contained in A , and this is our final contradiction. ■

Problems 2D

2D.1. Let $G = NA$, where $N \triangleleft G$, $\mathbf{C}_A(N) = 1$ and A is abelian.

- (a) If $\mathbf{F}(N) = 1$, show that $|A| < |N|$.
- (b) If $|N|$ and $|A|$ are coprime, show that $|A| < |N|$.

2D.2. Let $G = NA$, where $N \triangleleft G$, $\mathbf{C}_A(N) = 1$ and $A \cap N = 1$. If N is nontrivial and A is cyclic, show that $|A| < |N|$.

Split Extensions

3A

Given $N \triangleleft G$, a subgroup $H \subseteq G$ is a **complement** for N in G if $NH = G$ and $N \cap H = 1$, and if N has a complement in G , we say that G **splits** over N . Note that if H complements N in G , then $H \cong H/(N \cap H) \cong NH/N = G/N$, and thus all complements for N in G are isomorphic to G/N , and hence they are isomorphic to each other. An easy example where a group fails to split over some normal subgroup is $G = G_4$, the cyclic group of order 4, where N is the unique subgroup of order 2. It is clear that N is not complemented in G because if a complement existed, it would be isomorphic to G/N , which has order 2. But N is the only subgroup of order 2 in G , and of course, N is not a complement for itself.

If H complements N in G , then each element $g \in G$ is of the form $g = nh$, with $n \in N$ and $h \in H$, and this factorization is unique. (The uniqueness follows via an elementary computation, but if G is finite, an easier argument is to observe that $|G| = |N||H|$ and so the surjective map from pairs (n, h) to elements $nh \in G$ must also be injective.) It is also true, and for similar reasons, that each element of G is uniquely of the form hn , with $h \in H$ and $n \in N$. (To be specific, suppose that $g = nh$, and we wish to write $g = h'n'$, with $n' \in N$ and $h' \in H$. We have $g \in Nh = hN$ since $N \triangleleft G$, and thus we must have $h' = h$. The equation $hn' = nh$ then yields $n' = n^h$.)

If H complements N in G , then clearly, every conjugate of H in G also complements N . In general, however, a normal subgroup N of G may have nonconjugate complements, although as we have seen, all complements are isomorphic. An example where complements are not conjugate occurs in the Klein group $G = G_2 \times G_2$. If N is any one of the three subgroups of

order 2, then each of the other two subgroups of order 2 complements N , but these complements are not conjugate in G since G is abelian.

Our goal in this section is the following: given groups N and H , construct all (up to isomorphism) groups G having a normal subgroup N_0 complemented by a subgroup H_0 , where $N \cong N_0$ and $H \cong H_0$. (We refer to such a group as a **split extension** of H by N , but unfortunately, the literature is inconsistent on this point, and this group is sometimes also referred to as a split extension of N by H .) One such split extension, of course, is the (external) direct product $G = N \times H$, which is the set of ordered pairs (n, h) with $n \in N$ and $h \in H$, and where multiplication is componentwise. Here, we take $N_0 = \{(n, 1) \mid n \in N\}$ and $H_0 = \{(1, h) \mid h \in H\}$, and it is clear that $N_0 \cong N$, $H_0 \cong H$, $N_0 \triangleleft G$ and H_0 is a complement for N_0 in G . In this case, the complement H_0 also happens to be normal, and in general, it is easy to see that if the normal subgroup N_0 has a *normal* complement H_0 in G , then G is the (internal) direct product of N_0 and H_0 , and so $G \cong N \times H$. Our task, therefore, is to generalize the direct product construction sufficiently so that we get complements H_0 for N_0 in G , where H_0 is not necessarily normal in G . The desired construction is called the “semidirect product”.

Before we proceed, however, we digress briefly to discuss extensions that are not necessarily split. Given groups N and H , a group G is said to be an **extension** of H by N if there exists $N_0 \triangleleft G$ such that $N_0 \cong N$ and $G/N_0 \cong H$. Note that in our definition, the group preceded by the word “of” corresponds to the factor group, and the group preceded by “by” corresponds to the normal subgroup. As we mentioned, however, this use of prepositions is sometimes reversed in the literature, so readers should attempt to determine the precise meaning from the context.

There is a more fundamental ambiguity here. If G is an extension of H by N , then the normal subgroup N_0 of G such that $N_0 \cong N$ and $G/N_0 \cong H$ is not, in general, uniquely determined. In other words, G can be an extension of H by N in more than one way. In fact, it can happen that with one choice of the normal subgroup N_0 the extension is split, and with another it is not. Properly speaking, therefore, we really should say something like “ G is an extension of H by N with respect to the normal subgroup N_0 ”, and then it would make sense to ask if the extension is split.

Imagine that the “extension problem” could be completely solved. Suppose, in other words, that we knew how to construct (up to isomorphism) all extensions of H by N for given finite groups H and N . (We stress that this seems to be far from a realistic assumption.) Then, given that we know all simple groups, we could recursively construct all finite groups. To do this, assume that we have already constructed all groups of order less than n , where $n > 1$. Each group G of order n has some maximal normal subgroup,

say N . Since the factor group G/N is simple, every group of order n can be constructed as an extension of some (known) simple group S by some (already constructed) group N of order $n/|S|$. But even if we could do this, we would still be faced with the very difficult problem of deciding whether or not two groups of order n constructed in this way are isomorphic.

Returning to split extensions now, suppose that G is split over a normal subgroup N , and let H be a complement. Observe that H acts on N via conjugation in G , and in fact, conjugation by $h \in H$ induces an automorphism of N . If $H \triangleleft G$, then since $N \cap H = 1$, we know that H centralizes N , and so this conjugation action is trivial. If we wish to construct split extensions that are not merely direct products, therefore, we must consider nontrivial conjugation actions of H on N . Before proceeding with our construction, however, we show that no further information is needed; the subgroups N and H and the conjugation action of H on N completely determine G up to isomorphism.

To state the following uniqueness theorem, we introduce some convenient, but nonstandard notation. Consider isomorphic groups N and N_0 , where some specific isomorphism is given. For $n \in N$, we will write $n_0 \in N_0$ to denote the image of n under the given isomorphism, so that we can think of $()_0$ as the name of the isomorphism. We will use the same name $()_0$ to denote a given isomorphism from H to H_0 .

3.1. Lemma. *Let G and G_0 be groups, and suppose that $N \triangleleft G$ is complemented by H , and $N_0 \triangleleft G_0$ is complemented by H_0 . Assume that $N \cong N_0$ and $H \cong H_0$, where each of these isomorphisms is denoted by $()_0$, and suppose that*

$$(n^h)_0 = (n_0)^{h_0}$$

for all elements $n \in N$ and $h \in H$. Then there is a unique isomorphism from G to G_0 that extends the given isomorphisms $N \rightarrow N_0$ and $H \rightarrow H_0$.

Proof. Every element $g \in G$ is uniquely of the form hn , where $h \in H$ and $n \in N$, and so if we seek an isomorphism $\theta : G \rightarrow G_0$ that extends the given isomorphisms $N \rightarrow N_0$ and $H \rightarrow H_0$, we have no choice but to define $\theta(g) = \theta(hn) = \theta(h)\theta(n) = h_0n_0$. Since the decomposition $g = hn$ is unique, θ is well defined, and since every element $g_0 \in G_0$ has the form h_0n_0 with $h_0 \in H_0$ and $n_0 \in N_0$, it is clear that θ is surjective. It is injective because the decomposition $g_0 = h_0n_0$ is unique and h and n are the unique elements of H and N that map to h_0 and n_0 respectively.

It remains to show that θ is a homomorphism, and so we must compute $\theta((hn)(km))$, where $h, k \in H$ and $n, m \in N$. We have

$$(hn)(km) = hkk^{-1}nkm = (hk)(n^k m),$$

and so by definition, application of θ to this element yields

$$(hk)_0(n^k m)_0 = h_0 k_0 (n^k)_0 m_0 = h_0 k_0 (n_0)^{k_0} m_0 = h_0 n_0 k_0 m_0,$$

and this is exactly $\theta(hn)\theta(km)$, as required. ■

In order to construct all possible split extensions, we need to examine a little more abstractly the conjugation action of a group H on a group N . Recall that if H acts on a set Ω , then each element $h \in H$ induces a map $\sigma_h : \Omega \rightarrow \Omega$, defined by $\alpha \mapsto \alpha \cdot h$. Furthermore, σ_h is a permutation of Ω , and the map $h \mapsto \sigma_h$ is a homomorphism from H into the symmetric group $\text{Sym}(\Omega)$. It should be clear that the given action of H on Ω is completely determined by this homomorphism from H into $\text{Sym}(\Omega)$.

Suppose now that the set Ω of the previous paragraph happens to be a group, which we now call N . In this case, it is natural to require that for all elements $h \in H$, the map $\sigma_h : N \rightarrow N$ is actually an automorphism (and not just a permutation) of N . Of course, since this map is automatically both injective and surjective, it suffices to check that it is a homomorphism, or equivalently, that $(xy) \cdot h = (x \cdot h)(y \cdot h)$ for all $x, y \in N$.

Given groups H and N , we say that H **acts via automorphisms** on N if H acts on N as a set, and in addition, $(xy) \cdot h = (x \cdot h)(y \cdot h)$ for all $x, y \in N$ and $h \in H$. Just as an action of H on Ω determines and is determined by a homomorphism $H \rightarrow \text{Sym}(\Omega)$, so too, an action via automorphisms of H on N determines and is determined by a homomorphism $H \rightarrow \text{Aut}(N)$.

Perhaps the most natural examples of actions via automorphisms are where H is actually a subgroup of $\text{Aut}(N)$ and $n \cdot h$ is simply $(n)h$. Other examples of actions via automorphisms occur when both H and N are subgroups of some group G with $H \subseteq \mathbf{N}_G(N)$, and where the action is given by conjugation within G . In particular, the action of an arbitrary group G on itself by conjugation is an action via automorphisms.

It is common to use exponential notation instead of dots for actions via automorphisms, and so we write n^h instead of $n \cdot h$, where $n \in N$ and $h \in H$. This is natural for conjugation actions, of course, but it is potentially confusing for actions via automorphisms that are not defined by conjugation inside some given group. The following theorem, however, asserts that every action via automorphisms is essentially a conjugation action within an appropriate group. To some extent, therefore, this justifies the exponential notation for actions via automorphisms.

In order to state our result, we again use the notation $()_0$ to describe isomorphisms $N \rightarrow N_0$ and $H \rightarrow H_0$. Technically, this is ambiguous, however, because we will not assume that N and H are disjoint, and so if x lies in both of these groups, it may not be clear which isomorphism to apply

in order to compute x_0 . Nevertheless, we trust that this ambiguity will not cause confusion.

3.2. Theorem. *Let H and N be groups, and suppose that H acts on N via automorphisms. Then there exists a group G containing a normal subgroup $N_0 \cong N$, complemented by a subgroup $H_0 \cong H$, and such that for all $n \in N$ and $h \in H$, we have*

$$(n^h)_0 = (n_0)^{h_0}.$$

Here, $n^h \in N$ is the result of letting h act on n in the given action, while $(n_0)^{h_0} \in N_0$ is the result of conjugating n_0 by h_0 in G .

It follows by Lemma 3.1 that the group G of Theorem 3.2 is uniquely determined by N and H and the given action via automorphisms of H on N ; it is called the **semidirect product** of N by H with respect to the given action. Also, by Lemma 3.1, every group G with a normal subgroup N and complement H is isomorphic to a semidirect product of N by H , and so once we prove Theorem 3.2, it will be fair to say that we have constructed all possible split extensions (up to isomorphism).

A common notation for a semidirect product G of N by H is $G = N \rtimes H$. (This notation is incomplete, of course, because it fails to mention the specific action via automorphisms that is essential in the definition. When we construct a group $G = N \rtimes H$, we should always specify the action.) Note that the semidirect product is a direct product if and only if $H_0 \triangleleft G$, and this happens precisely when the conjugation action of H_0 on N_0 is trivial, or equivalently, when the original action of H on N is trivial.

We offer a mnemonic for the correct use of the symbol “ \rtimes ”, which looks like “ \times ” with an extra little vertical line on the right. If $G = N \rtimes H$, the little line reminds us that from the point of view of H , the semidirect product can be different from a direct product since H may not be normal. But N is normal in G , and so from the point of view of N , the semidirect product resembles a direct product.

We often identify N with N_0 and H with H_0 via the isomorphisms $x \mapsto x_0$, so that the semidirect product $G = N \rtimes H$ can be viewed as a split extension with $N \triangleleft G$, $NH = G$ and $N \cap H = 1$, and where the original action via automorphisms of H on N is just the conjugation action within G . We stress, however, that that this identification is not always a good idea, and it can lead to confusion. Consider, for example, an arbitrary group G and let $\Gamma = G \rtimes G$ with respect to the natural conjugation action of G on itself. (Somewhat remarkably, it turns out that $\Gamma \cong G \times G$ for all groups G .)

It is seldom necessary or appropriate to refer to the proof of Theorem 3.2. In other words, the specific construction of the semidirect product is largely

irrelevant. The point here is that given the three ingredients: a group N , a group H and an action via automorphisms of H on N , there is a group G , which is unique up to isomorphism and satisfies the conclusions of Theorem 3.2. It is usually unnecessary to know exactly how G is constructed. (Indeed, there is more than one way to prove Theorem 3.2, which means that there is more than one possible construction for the semidirect product.) In order to emphasize this point, we give a few applications of semidirect products before we present the construction.

Recall that in Chapter 2, we defined the dihedral group $D = D_{2n}$ as a group having a nontrivial cyclic subgroup C of order n such that all elements of $D - C$ are involutions. We argued using geometric reasoning that such a group actually exists when $n \geq 3$. Using semidirect products, we can give a cleaner construction of the dihedral group D_{2n} and some related groups.

Let A be an arbitrary abelian group, and let $T = \langle t \rangle$ be cyclic of order 2. Since t is the only nonidentity element of T , we can define an action of T on A by setting $x^t = x^{-1}$ for all $x \in A$. (Since $t^2 = 1$ and $(x^{-1})^{-1} = x$, this is clearly a genuine action.) Because A is abelian, we have $(xy)^{-1} = x^{-1}y^{-1}$, and so our action of T on A is an action via automorphisms. Now let $G = A \rtimes T$ with respect to this action, and identify (as we may) A and T with the corresponding subgroups of the semidirect product G . Then $A \triangleleft G$ and A is complemented by T in G , and thus $|G : A| = |T| = 2$, and we have $|G| = 2|A|$. Also, the equation $x^t = x^{-1}$, can be viewed as a statement about conjugation in the semidirect product G . Now every element g of $G - A$ lies in the coset At , and so $g = at$ for some element $a \in A$. In particular, $g^2 = atat = aa^t = aa^{-1} = 1$, and so all elements of $G - A$ are involutions. In other words, G is a generalized dihedral group and in particular, if A is cyclic of order n , then G is dihedral of order $2n$.

We can also use the semidirect product construction to prove things. At first glance, the following may seem almost obvious, but its proof depends on nontrivial facts from Chapter 2.

3.3. Corollary (Horosevskii). *Let $\sigma \in \text{Aut}(G)$, where G is a nontrivial finite group. Then the order $o(\sigma)$ of σ is less than $|G|$.*

Proof. Let $A = \langle \sigma \rangle$, so that A is a cyclic subgroup of $\text{Aut}(G)$ and $|A| = o(\sigma)$. Since $A \subseteq \text{Aut}(G)$, there is a natural action of A on G by automorphisms, and we construct the semidirect product $\Gamma = G \rtimes A$ with respect to this action. As usual, we identify G and A with subgroups of Γ , so that $G \triangleleft \Gamma$ and A is a complement for G . Also, the conjugation action of A on G in Γ is the original action. Furthermore, since by definition, nonidentity automorphisms of G act nontrivially, it follows that no nonidentity element of A acts trivially on G by conjugation in Γ . In other words, $A \cap \mathbf{C}_\Gamma(G) = 1$.

Since G is nontrivial and A is cyclic, Lucchini's theorem (2.20) applies in Γ , and we deduce that $|A : K| < |\Gamma : A|$, where $K = \text{core}_\Gamma(A)$. But $K \cap G \subseteq A \cap G = 1$, and both K and G are normal in Γ , and thus $K \subseteq A \cap \mathbf{C}_\Gamma(G) = 1$. Thus $o(\sigma) = |A| = |A : K| < |\Gamma : A| = |G|$, as required. ■

Somewhat similarly, we have the following.

3.4. Corollary. *Let P be an abelian p -subgroup of $\text{Aut}(G)$, where G is a finite group of order not divisible by the prime p . Then P has a regular orbit on G . In particular, if G is nontrivial, then $|P| < |G|$.*

Recall that if a group P acts on a set Ω , then a P -orbit A in Ω is regular if $|A| = |P|$, or equivalently (by the fundamental counting principle) the stabilizer in P of an element of A is trivial. Also, in the situation of the corollary, if $P > 1$ and A is a regular P -orbit, then A does not contain the identity of G , and so $|G| \geq 1 + |A| > |P|$. This shows that the last sentence of Corollary 3.4 will follow once the existence of a regular P -orbit is established.

Proof of Corollary 3.4. Since $P \subseteq \text{Aut}(G)$, there is a natural action of P on G via automorphisms. Let $\Gamma = G \rtimes P$ with respect to this action, and as usual, identify P and G with subgroups of Γ . Then $|\Gamma : P| = |G|$ is not divisible by p , and so $P \in \text{Syl}_p(\Gamma)$. Also, the conjugation action of P on G in Γ is the original action, and since P consists of automorphisms, only the identity in P acts trivially. It follows that $P \cap \mathbf{C}_\Gamma(G) = 1$.

Now $\mathbf{O}_p(\Gamma) \subseteq P$, and so $\mathbf{O}_p(\Gamma) \cap G = 1$. Also, both G and $\mathbf{O}_p(\Gamma)$ are normal in Γ , and hence they centralize each other, and we have $\mathbf{O}_p(\Gamma) \subseteq P \cap \mathbf{C}_\Gamma(G) = 1$. Since the Sylow subgroup P is abelian, it follows by Brodkey's theorem (1.37) that $\mathbf{O}_p(\Gamma)$ is an intersection of two Sylow p -subgroups. Replacing them by conjugates if necessary, we can assume that one of these Sylow subgroups is P , and the other is P^x for some element $x \in \Gamma$. We thus have $P \cap P^x = \mathbf{O}_p(\Gamma) = 1$.

We can write $x = ug$, with $u \in P$ and $g \in G$, and thus $P^x = P^{ug} = P^g$, and we have $P \cap P^g = 1$. We claim that the P -orbit in G that contains g is regular, and this will complete the proof. It suffices to show that the stabilizer in P of g is trivial, but since the action of P on G is conjugation in Γ , what we want to establish is that $\mathbf{C}_P(g) = 1$. We have $\mathbf{C}_P(g) = \mathbf{C}_P(g)^g$, and hence $\mathbf{C}_P(g) \subseteq P \cap P^g = 1$, as wanted. ■

A comparison of the previous two corollaries suggests that perhaps whenever A is a cyclic subgroup of $\text{Aut}(G)$, there is always a regular A -orbit in G . If that were true, it would be a strong form of Corollary 3.3, but alas, it is false.

Finally, we are ready to prove Theorem 3.2 by actually constructing the semidirect product $\Gamma = N \rtimes H$. A common way to do this, by analogy with the construction of the external direct product, is to define an appropriate multiplication on the set of ordered pairs (h, n) with $h \in H$ and $n \in N$. One tedious, but necessary, step using this construction is to check that the defined multiplication is associative. We choose to use a different approach, which avoids checking associativity. This is accomplished by working in an appropriate symmetric group, where, of course, associativity is automatic.

Proof of Theorem 3.2. Let Ω be the set of ordered pairs (k, m) , where $k \in H$ and $m \in N$. It is trivial to check that actions of N and of H on Ω are defined by the following:

$$(k, m) \cdot n = (k, mn) \quad \text{and} \quad (k, m) \cdot h = (kh, m^h),$$

where $(k, m) \in \Omega$ and $n \in N$ and $h \in H$. Here, of course, m^h is the result of letting h act on m in the given action via automorphisms of H on N .

Since N acts on Ω , we have a natural homomorphism $n \mapsto n_0$ from N into the symmetric group $\text{Sym}(\Omega)$, where n_0 is the permutation $\alpha \mapsto \alpha \cdot n$ for $\alpha \in \Omega$. Write $N_0 = \{n_0 \mid n \in N\}$, so that $N_0 \subseteq \text{Sym}(\Omega)$ is a subgroup and $(\)_0$ is a surjective homomorphism from N to N_0 . If $n_0 = 1$, then $(k, m) \cdot n = (k, m)$ for all $k \in H$ and $m \in N$, and in particular, $(1, 1) \cdot n = (1, n)$. It follows that $n = 1$, and so the homomorphism $(\)_0$ has trivial kernel. It is thus an isomorphism from N onto N_0 .

Similarly, if $h \in H$, write $h_0 \in \text{Sym}(\Omega)$ to denote the map $\alpha \mapsto \alpha \cdot h$, and let $H_0 = \{h_0 \mid h \in H\}$. Then $H_0 \subseteq \text{Sym}(\Omega)$ is a subgroup and $(\)_0$ is a homomorphism from H onto H_0 . (As before, we are using the notation $(\)_0$ for two different maps.) If $h_0 = 1$, then $(1, 1) \cdot h = (h, 1^h)$, and thus $h = 1$ and $(\)_0$ is an isomorphism from H onto H_0 .

Next, we argue that $(n^h)_0 = (n_0)^{h_0}$ for all $n \in N$ and $h \in H$. Since this is a statement about elements of $\text{Sym}(\Omega)$, it suffices to check that both $(n^h)_0$ and $(n_0)^{h_0}$ have the same effect on each element of Ω . We have

$$(k, m)(n^h)_0 = (k, m) \cdot n^h = (k, mn^h).$$

Also,

$$\begin{aligned} (k, m)(n_0)^{h_0} &= (k, m)(h_0)^{-1}n_0h_0 = (((k, m) \cdot h^{-1}) \cdot n) \cdot h \\ &= ((kh^{-1}, m^{h^{-1}}) \cdot n) \cdot h \\ &= (kh^{-1}, m^{h^{-1}}n) \cdot h \\ &= (k, mn^h), \end{aligned}$$

where the last equality holds because $(m^{h^{-1}}n)^h = mn^h$. (This is valid because the action of H on N is an action via automorphisms.) We conclude

that $(n^h)_0 = (n_0)^{h_0}$ as claimed, and in particular, $H_0 \subseteq \mathbf{N}_{\text{Sym}(\Omega)}(N_0)$. We can now define $G = N_0 H_0$, so that G is a subgroup of $\text{Sym}(\Omega)$, and $N_0 \triangleleft G$. All that remains is to show that H_0 is a complement for N_0 in G . Since by definition, $G = N_0 H_0$, it suffices to check that $N_0 \cap H_0 = 1$. To this end, suppose that $n_0 = h_0$ with $n \in N$ and $h \in H$. Then

$$(h, 1) = (1, 1) \cdot h = (1, 1) h_0 = (1, 1) n_0 = (1, 1) \cdot n = (1, n),$$

and it follows that $h = 1$. Thus $n_0 = h_0 = 1$, and the proof is complete. ■

We close this section with a description of the wreath product, which is useful for constructing examples and counterexamples. The ingredients here are two groups G and H , and a set Ω , acted on by G . Let B be the set of all functions from Ω into H , and make B into a group by defining multiplication pointwise. Thus if $f, g \in B$, then fg is defined by the formula $(fg)(\alpha) = f(\alpha)g(\alpha)$ for $\alpha \in \Omega$. It is trivial to check that B is a group, and in fact, B is really just the external direct product of $|\Omega|$ copies of H .

The action of G on Ω induces an action via automorphisms of G on B . If we view B as a direct product, the action of G can be described simply as a permutation of coordinates, but it is useful to be more precise. Given $f \in B$ and $x \in G$, the function f^x on Ω is defined so that $f^x(\alpha \cdot x) = f(\alpha)$, or equivalently, $f^x(\alpha) = f(\alpha \cdot x^{-1})$. (It is routine to show that this defines an action via automorphisms, and we omit the proof.)

Now let $W = B \rtimes G$ with respect to this action. Then W is the **wreath product** of H with G , and B , viewed as a subgroup of W , is called the **base group** of the wreath product. It is common to write $W = H \wr G$, but of course, this notation for the wreath product is defective in that it does not mention the set Ω or the action of G on Ω . If G is given as an abstract group, and no set Ω is mentioned, then it is understood that $H \wr G$ is constructed using the “regular” action of G . This means that we take $\Omega = G$, with G acting by right multiplication. Sometimes, this is referred to as the **regular wreath product** of H by G .

Problems 3A

3A.1. Let C be a cyclic group of order n divisible by 8, and let z be the unique involution in C .

- Show that C has a unique automorphism σ such that $c^\sigma = c^{-1}z$ for every generator c of C , and show that σ has order 2.
- Let $S = C \rtimes \langle \sigma \rangle$, so that $|S| = 2|C|$. Show that half of the elements of $S - C$ have order 2 and that the other half have order 4.
- Show that the elements of order 2 in $S - C$ form a single conjugacy class of S , and similarly for the elements of order 4.

Note. The group S is the **semidihedral** group SD_{2n} , although in the literature, the word “semidihedral” is usually reserved for the case where n is a power of 2, and there seems to be no standard name for other members of this family of groups.

3A.2. Let S and C be as in the previous problem, and let B be the subgroup of index 2 in G . Show that the elements of order 4 in $S - C$ form a coset of B , and let Q be the union of this coset and B . Show that Q is a subgroup of order n .

Note. Since all elements of $Q - B$ have order 4, the involution in B is the unique involution in Q . The group Q is the **generalized quaternion** group Q_n . (The phrase “generalized quaternion” is often restricted to the case where the order n is a power of 2. The undecorated word “quaternion” is usually reserved for Q_8 .)

3A.3. Let p be a prime, and suppose that m is a divisor of $p-1$ with $m > 1$. Show that there exists a group G of order pm with a normal subgroup P of order p , and such that G/P is cyclic and $\mathbf{Z}(G) = 1$.

3A.4. Let q be a power of a prime p . Show that there exists a group G of order $q(q-1)$ with a normal elementary abelian subgroup of order q and such that all elements of order p in G are conjugate.

Hint. Let F be a field of order q and observe that the multiplicative group of F acts via automorphisms on the additive group of F .

3A.5. Let G be an arbitrary finite group. Show that $G \rtimes G \cong G \times G$, where the semidirect product is constructed using the natural action of G on itself by conjugation.

3A.6. Recall that a group action is faithful if the only group element that fixes all points is the identity. Let P be a p -group acting faithfully via automorphisms on a group G with order not divisible by p . Show that P acts faithfully on some P -orbit A in G .

Hint. Use Theorem 1.38, the generalized Brodkey theorem.

3A.7. Let $\sigma \in \text{Aut}(G)$, and suppose that at most two prime numbers divide $o(\sigma)$. Show that $\langle \sigma \rangle$ has a regular orbit on G .

3A.8. Let C be cyclic of order pqr , where p, q and r are distinct odd primes.

- (a) Let $s \in \{p, q, r\}$. Show that $\text{Aut}(G)$ contains a unique involution α fixing elements of G of order s and inverting elements of prime orders different from s .

- (b) Applying (a) three times, with $s = p$, $s = q$ and $s = r$, we get three involutions in $\text{Aut}(C)$. Show that these together with the identity form a subgroup $K \subseteq \text{Aut}(C)$ of order 4.
- (c) Let $G = C \rtimes K$ with the natural action, and let σ be the inner automorphism of G induced by a generator of C . Show that $\langle \sigma \rangle$ has no regular orbit on G .

3A.9. Let $W = H \wr G$ be a wreath product constructed with respect to a transitive action of G on some set Ω . Let B be the corresponding base group.

- (a) Show that $C_B(G)$ is the set of constant functions from Ω into H .
- (b) Now assume that W is the regular wreath product, so that $\Omega = G$. Let $C \subseteq G$ be an arbitrary subgroup. Show that there exists $b \in B$ such that $C_G(b) = C$.

3A.10. Given a finite group H and a prime p , show that there exists a group G having a normal abelian p -subgroup A such that G splits over A , where $G/A \cong H$ and $A = C_G(A)$.

3B

The Schur-Zassenhaus theorem is a powerful result that guarantees that a finite group G always splits over a normal Hall subgroup N . (Recall that by definition, N is a Hall subgroup of G if $|N|$ and $|G : N|$ are relatively prime.)

The Schur-Zassenhaus theorem says even more: if N is a normal Hall subgroup of G , then all complements for N in G are conjugate. Unfortunately, however, the proof of the conjugacy part of the Schur-Zassenhaus theorem requires the additional hypothesis that either N or G/N is solvable. (We review the definition and basic properties of solvable groups later in this section.) If we are willing to apply the very deep Feit-Thompson odd-order theorem, however, we see that this solvability requirement is not really a limitation. This is because the assumption that N and G/N have coprime orders guarantees that at least one of these groups has odd order, and hence is solvable by the Feit-Thompson theorem. The conjugacy part of the Schur-Zassenhaus theorem is therefore true unconditionally, although no direct or elementary proof of this is known. For the purposes of this book, we will *assume* solvability when appropriate, and we will generally not appeal to the Feit-Thompson theorem.

Of course, if H is a complement for a normal subgroup N in G , then $|H| = |G : N|$. It is useful to observe that in the situation of the Schur-Zassenhaus theorem, where $|N|$ and $|G : N|$ are coprime, the converse of this

statement is also true. If $H \subseteq G$ and $|H| = |G : N|$, then H is a complement for N in G . To see this, observe that $|H| = |G : N|$ is coprime to $|N|$, and thus $N \cap H = 1$. From this, we deduce that $|NH| = |N||H| = |G|$, and hence $NH = G$, and indeed H is a complement for N as claimed.

Although several proofs of the Schur-Zassenhaus theorem are known, the key step in all of them is to establish the result in the case where N is abelian. What are essentially routine tools can then be used to reduce the general situation to this case. (Of course, the assumption for the conjugacy part that either N or G/N is solvable is used in the reduction.) Our first major goal, therefore, is the following.

3.5. Theorem. *Let $N \triangleleft G$, where G is a finite group, and assume that N is abelian and that $|N|$ and $|G : N|$ are coprime. Then N is complemented in G , and all complements are conjugate.*

If our goal were to find a certain *normal* subgroup in G , we might proceed by constructing an appropriate homomorphism from G , and then considering its kernel. But we need a complement for N , which will not generally be normal. We will construct it as the “kernel” of a certain kind of distorted homomorphism.

Let G act via automorphisms on N , and consider a map $\varphi : G \rightarrow N$. Then φ is a **crossed homomorphism** if $\varphi(xy) = \varphi(x)^y \varphi(y)$ for all elements x and y in G . (Of course, the exponent y here refers to the given action via automorphisms of G on N .)

If the action of G on N is trivial, which means that $n^g = n$ for all $n \in N$ and $g \in G$, then a crossed homomorphism from G to N is simply an ordinary homomorphism. But we will see that there are also interesting examples when the action is nontrivial. For example, let G be an arbitrary group and suppose $N \triangleleft G$, so that G acts on N by conjugation. Now fix an element $n \in N$, and define the map $\varphi : G \rightarrow N$ by setting $\varphi(x) = [x, n]$. (Recall that $[x, n]$ is the commutator of x and n , which, by definition, is the element $x^{-1}n^{-1}xn = (n^{-1})^x n$.) Since $n \in N \triangleleft G$, it is clear that $\varphi(x) = [x, n]$ lies in N , as claimed. Now $\varphi(xy) = [xy, n]$, and an easy computation, which we omit, establishes the identity $[xy, n] = [x, n]^y [y, n]$. Thus $\varphi(xy) = \varphi(x)^y \varphi(y)$, and so φ is a crossed homomorphism.

By analogy with kernels of ordinary homomorphisms, we define the **kernel** of a crossed homomorphism $\varphi : G \rightarrow N$ to be the subset $\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\}$. The following establishes a few basic facts about crossed homomorphisms and their kernels.

3.6. Lemma. *Let G and N be groups, and suppose that G acts via automorphisms on N . Let $\varphi : G \rightarrow N$ be a crossed homomorphism with kernel K . The following then hold.*

- (a) $\varphi(1) = 1$.
- (b) K is a subgroup of G .
- (c) If $x, y \in G$, then $\varphi(x) = \varphi(y)$ if and only if $Kx = Ky$.
- (d) $|G : K| = |\varphi(G)|$.

Proof. We have

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)^1 \varphi(1) = \varphi(1)^2,$$

and it follows that $1 = \varphi(1)$. This establishes (a) and shows that K is nonempty. If $k \in K$, we have

$$1 = \varphi(1) = \varphi(kk^{-1}) = \varphi(k)^{k^{-1}} \varphi(k^{-1}) = \varphi(k^{-1}),$$

where the last equality holds because $\varphi(k) = 1$ and $1^g = 1$ for all elements $g \in G$. Thus $k^{-1} \in K$, and K is closed under inverses. Also, if $x, y \in K$, then

$$\varphi(xy) = \varphi(x)^y \varphi(y) = 1^y 1 = 1,$$

and so $xy \in K$, and hence K is a subgroup, proving (b).

Now if $x, y \in G$ and $Kx = Ky$, we can write $y = kx$ with $k \in K$. Then

$$\varphi(y) = \varphi(kx) = \varphi(k)^x \varphi(x) = \varphi(x),$$

where the last equality holds because $\varphi(k) = 1$.

Conversely, if $\varphi(x) = \varphi(y)$, we compute that

$$\varphi(xy^{-1}) = \varphi(x)^{y^{-1}} \varphi(y) = \varphi(y)^{y^{-1}} \varphi(y) = \varphi(yy^{-1}) = \varphi(1) = 1,$$

and so $xy^{-1} \in K$. Thus $x \in Ky$ and $Kx = Ky$, as wanted. Finally, since φ is constant on right cosets of K and takes distinct values on distinct right cosets, it follows that $|\varphi(G)|$ is exactly the number of such cosets. This proves (d). ■

Our next task is to construct an appropriate crossed homomorphism from a finite group G into an abelian normal subgroup N . To do this, we consider the **transversals** for N in G . These are the subsets T of G constructed by choosing exactly one member from each coset of N in G . (Note that since N is normal, left cosets and right cosets are the same, so we need not specify “left transversal” or “right transversal”.) Since right multiplication by an element $g \in G$ permutes the right cosets of an arbitrary subgroup of G , it follows that if T is a transversal for N , then Tg is also a transversal for N . We write \mathcal{T} to denote the set of all transversals for N in G .

If $x, y \in G$, write $x \equiv y$ if x and y lie in the same coset of N . Thus $x \equiv y$ if and only if $Nx = Ny$, or equivalently, $xN = yN$. If $S, T \in \mathcal{T}$, the relation $s \equiv t$ for $s \in S$ and $t \in T$ defines a natural bijection between S and

T , and we use this bijection to define an element of N that we call $d(S, T)$. (In some sense, $d(S, T)$ measures the difference between S and T .) We set

$$d(S, T) = \prod_{s \equiv t} s^{-1}t,$$

where the product runs over all $s \in S$ and $t \in T$ such that $s \equiv t$. Of course, if $s \equiv t$, then $sN = tN$, and so $s^{-1}t \in N$, and hence each factor in the product lies in N . Also, because we are assuming that N is abelian, the order in which the factors appear is irrelevant, and thus $d(S, T)$ is a well defined element of N .

Some elementary properties of the function d are given in the following.

3.7. Lemma. *Let N be abelian and normal in a finite group G , and let S , T and U be transversals for N . Then using the notation defined above, the following hold.*

- (a) $d(S, T)d(T, U) = d(S, U)$.
- (b) $d(Sg, Tg) = d(S, T)^g$ for all $g \in G$.
- (c) $d(S, Sn) = n^{|G:N|}$ for all $n \in N$.

Proof. If $s \equiv t$ and $t \equiv u$ for $s \in S$, $t \in T$ and $u \in U$, then $Ns = Nt = Nu$, and so $s \equiv u$. Since $(s^{-1}t)(t^{-1}u) = s^{-1}u$ and the order of factors in the abelian group N is irrelevant, (a) follows.

Now let $g \in G$. If $s \equiv t$, then $Ns = Nt$, and so $Nsg = Ntg$, and $sg \equiv tg$. The factor $(sg)^{-1}(tg)$ of the product defining $d(Sg, Tg)$ is equal to $(s^{-1}t)^g$, and assertion (b) follows.

Finally, if $n \in N$, we have $sN = (sn)N$, and so $s \equiv sn$. Each factor $s^{-1}(sn)$ of the product defining $d(S, Sn)$ equals n , and so (c) follows because $|S| = |G : N|$. ■

We are now ready to prove the case of the Schur-Zassenhaus theorem where N is an abelian normal Hall subgroup of G .

Proof of Theorem 3.5. Fix an arbitrary transversal T for N in G , and define $\theta : G \rightarrow N$ by setting $\theta(g) = d(T, Tg)$. We argue first that θ is a crossed homomorphism with respect to the conjugation action of G on N . If $x, y \in G$, then using Lemma 3.7(a,b), we compute that

$$d(T, Txy) = d(T, Ty)d(Ty, Txy) = d(T, Ty)d(T, Tx)^y,$$

and so $\theta(xy) = \theta(y)\theta(x)^y$. This, of course, is equal to $\theta(x)^y\theta(y)$ since N is abelian, and so θ is a crossed homomorphism, as claimed.

For $n \in N$, we have $\theta(n) = d(T, Tn) = n^{|G:N|}$ by Lemma 3.7(c). Since we are assuming that $|N|$ and $|G : N|$ are coprime, however, the map $x \mapsto x^{|G:N|}$ is a permutation of the elements of N . (One way to see this is to observe

that this map has an inverse: the map $x \mapsto x^k$, where the integer k is chosen so that $k|G : N| \equiv 1 \pmod{|N|}$.) It follows that θ maps N onto N , and in particular, $\theta(G) = N$. Now let $H = \ker(\theta)$, so that H is a subgroup by Lemma 3.6(b). Also, $|N| = |\theta(G)| = |G : H|$ by Lemma 3.6(d), and hence $|N||H| = |G|$ and $|H| = |G : N|$. We have already observed that since $|N|$ and $|G : N|$ are coprime, this is sufficient to guarantee that H is a complement for N , as wanted.

Now suppose that K is an arbitrary complement for N in G . Since $NK = G$, we see that every coset of N in G contains an element of K , and in fact, each coset of N contains a unique element of K because $N \cap K = 1$. Thus K is a transversal for N , and we let $m = d(K, T) \in N$. We saw that the restriction of θ to N is the map $x \mapsto x^{|G:N|}$, which is surjective, and so we can find $n \in N$ such that $\theta(n) = m$, and thus $\theta(n^{-1}) = m^{-1}$.

To complete the proof, we show that $K^n = H$. Since $|K| = |G : N| = |H|$, it suffices to show that $K^n \subseteq H$, or equivalently, that $\theta(k^n) = 1$ for all $k \in K$. (Recall that $H = \ker(\theta)$.) First, observe that if $k \in K$, then

$$m^k = d(K, T)^k = d(Kk, Tk) = d(K, Tk) = d(K, T)d(T, Tk) = m\theta(k),$$

and so $1 = (m^k)^{-1}m\theta(k) = (m^k)^{-1}\theta(k)m$. We have

$$\begin{aligned} \theta(k^n) &= \theta(n^{-1}kn) = \theta(n^{-1}k)^n\theta(n) = \theta(n^{-1}k)m \\ &= \theta(n^{-1})^k\theta(k)m \\ &= (m^{-1})^k\theta(k)m, \end{aligned}$$

where we were able to drop the exponent n in the third equality because N is abelian. Thus $\theta(k^n) = 1$, and we are done. ■

Next, we prove the existence part of the Schur-Zassenhaus theorem without assuming that the normal Hall subgroup is abelian.

3.8. Theorem. *Let $N \triangleleft G$, where G is a finite group and $|N|$ and $|G : N|$ are coprime. Then N is complemented in G .*

Proof. We proceed by induction on $|G|$. Suppose that there exists a subgroup $K < G$ such that $NK = G$. Then $|K : K \cap N| = |G : N|$ is coprime to $|N|$, and hence it is also coprime to $|K \cap N|$. Since $K \cap N \triangleleft K$, the inductive hypothesis guarantees that $K \cap N$ is complemented in K , and we choose a complement H . Then $|H| = |K : K \cap N| = |G : N|$ and as we have seen, this guarantees that H is a complement for N in G .

We may thus suppose that there is no proper subgroup K of G such that $NK = G$, and so in particular, N must be contained in every maximal subgroup of G . In other words, $N \subseteq \Phi(G)$, the Frattini subgroup, and so

N is nilpotent. Also, we can assume that $N > 1$ or else G is the desired complement for N in G .

Now let $Z = \mathbf{Z}(N)$, and observe that $1 < Z \triangleleft G$. Working in the group $\overline{G} = G/Z$, we see that $|\overline{G} : \overline{N}| = |G : N|$ is coprime to $|N|$ and hence is also coprime to $|\overline{N}|$. It follows by the inductive hypothesis that \overline{G} splits over \overline{N} , and we let \overline{K} be a complement. Then $\overline{G} = \overline{N} \overline{K} = \overline{N} \overline{K}$, and hence $G = NK$. It follows by the earlier part of the proof that K cannot be proper, and we have $K = G$. Because \overline{K} is a complement for \overline{N} , however, their intersection must be the trivial subgroup \overline{Z} . Thus

$$\overline{Z} = \overline{N} \cap \overline{K} = \overline{N} \cap \overline{G} = \overline{N},$$

and hence $N = Z$ is abelian. The result now follows via Theorem 3.5. ■

As we said, it is necessary to assume that either N or G/N is solvable in order to prove the conjugacy part of the Schur-Zassenhaus theorem. Perhaps, therefore, a review of some basic facts about solvable groups would be appropriate, and so we begin with the definition. A (not necessarily finite) group G is **solvable** if there exist normal subgroups N_i such that

$$1 = N_0 \subseteq N_1 \subseteq N_2 \subseteq \cdots \subseteq N_r = G,$$

where N_i/N_{i-1} is abelian for $1 \leq i \leq r$. (In particular, all abelian groups are solvable since if G is abelian, we can take $N_0 = 1$ and $N_1 = G$.) A finite chain of nested normal subgroups of G , extending from the trivial subgroup to the whole group, is called a **normal series** for G , and thus G is solvable precisely when it has a normal series with abelian factors.

Recall that the **commutator subgroup** (or **derived subgroup**) of an arbitrary group G is the subgroup G' generated by all commutators $[x, y] = x^{-1}y^{-1}xy$, with $x, y \in G$. Since $[x, y] = 1$ if and only if x and y commute, we see that G is abelian if and only if $G' = 1$. Also, if $\varphi : G \rightarrow H$ is a surjective homomorphism, then φ maps the set of commutators in G onto the set of commutators in H , and thus $\varphi(G') = H'$. It follows that H is abelian if and only if $G' \subseteq \ker(\varphi)$, and in particular, if $N \triangleleft G$, then G/N is abelian precisely when $G' \subseteq N$. In other words, the derived subgroup of G is the unique smallest normal subgroup of G having an abelian factor group.

The subgroup $(G')'$ is usually denoted G'' , and its derived subgroup, is G''' . This notation rapidly gets unwieldy, however, and so we write $G^{(n)}$ for the n th derived subgroup. In other words, $G^{(0)} = G$ and for $n > 0$, we define $G^{(n)} = (G^{(n-1)})'$. The subgroups $G^{(n)}$ are characteristic, and they constitute the **derived series** of G .

The connection with solvability is the following.

3.9. Lemma. *A group G is solvable if and only if $G^{(m)} = 1$ for some integer $m \geq 0$.*

Proof. If G is solvable, choose normal subgroups N_i such that

$$1 = N_0 \subseteq \cdots \subseteq N_r = G,$$

where N_i/N_{i-1} is abelian for $1 \leq i \leq r$, and thus $(N_i)' \subseteq N_{i-1}$ for subscripts in this range. It is clear, however, that if $H \subseteq G$, then $H' \subseteq G'$, and thus since $G' = (N_r)' \subseteq N_{r-1}$, we have (if $r \geq 2$) that $G'' \subseteq (N_{r-1})' \subseteq N_{r-2}$. Continuing like this, we get $G^{(m)} \subseteq N_{r-m}$ for $m \leq r$, and in particular, $G^{(r)} \subseteq N_0 = 1$.

Conversely, suppose that $G^{(m)} = 1$. Since the subgroups $G^{(i)}$ are characteristic in G , they are certainly normal, and we have the normal series

$$1 = G^{(m)} \subseteq G^{(m-1)} \subseteq \cdots \subseteq G^{(0)} = G.$$

The factors here are abelian, and so G is solvable. ■

The characterization of solvability in terms of the derived series allows us to prove a number of useful facts.

3.10. Lemma. *Let G be an arbitrary group.*

- (a) *If $H \subseteq G$, then $H^{(m)} \subseteq G^{(m)}$ for all $m \geq 0$.*
- (b) *If $\varphi : G \rightarrow H$ is a surjective homomorphism, then $\varphi(G^{(m)}) = H^{(m)}$ for all $m \geq 0$.*
- (c) *If G is solvable and $H \subseteq G$, then H is solvable.*
- (d) *If G is solvable and $N \triangleleft G$, then G/N is solvable.*
- (e) *Let $N \triangleleft G$ and suppose that N and G/N are solvable. Then G is solvable.*

Proof. If $H \subseteq G$, then $H' \subseteq G'$ and (a) follows by repeating this observation. Similarly, (b) follows by repeated application of the fact that $\varphi(G') = H'$ if $\varphi : G \rightarrow H$ is a surjective homomorphism.

Now suppose that G is solvable, so that $G^{(n)} = 1$ for some integer n . If $H \subseteq G$, then $H^{(n)} \subseteq G^{(n)} = 1$ by (a), and thus H is solvable, proving (c). If $\varphi : G \rightarrow H$ is a surjective homomorphism, then $H^{(n)} = \varphi(G^{(n)}) = \varphi(1) = 1$, and H is solvable. In particular, if $N \triangleleft G$ and we take φ to be the canonical homomorphism of G onto G/N , we obtain (d).

For (e), let $H = G/N$ and again let $\varphi : G \rightarrow H$ be the canonical homomorphism. Since H is solvable, $\varphi(G^{(n)}) = H^{(n)} = 1$ for some integer n , and thus $G^{(n)} \subseteq \ker(\varphi) = N$. Also, since N is solvable, we have $N^{(m)} = 1$ for some integer m , and thus $G^{(m+n)} = (G^{(n)})^{(m)} \subseteq N^{(m)} = 1$, and thus G is solvable. ■

Recall that an abelian p -group P is elementary abelian if $x^p = 1$ for all $x \in P$. A useful fact about solvable groups is that a minimal normal subgroup of a finite solvable group must be an elementary abelian p -group for some prime p . The following is a slightly more general version of this.

3.11. Lemma. *Let M be a solvable minimal normal subgroup of an arbitrary group G . Then M is abelian, and if M is finite, it is an elementary abelian p -group for some prime p .*

Proof. Since M is solvable, its derived series must eventually reach 1, and thus since $M > 1$, we conclude that $M' < M$. But M' is characteristic in M , and hence it is normal in G . It follows by the minimality of M that $M' = 1$, and thus M is abelian, as wanted. Now assume that M is finite, and let $u \in M$ be an element of prime order, say p . Since M is abelian, the set $S = \{x \in M \mid x^p = 1\}$ is a characteristic subgroup of M and hence it is normal in G . Also, $S > 1$ since $u \in S$, and thus $S = M$ by the minimality of M . This completes the proof. ■

Finally, we mention that the **derived length** of a solvable group G is the smallest integer n such that $G^{(n)} = 1$. (Thus, for example, a solvable group has derived length 1 precisely when it is nontrivial and abelian.) The proof of Lemma 3.10 shows that subgroups and homomorphic images of a solvable group with derived length n have derived lengths at most n . Also, if $N \triangleleft G$, where N is solvable with derived length m and G/N is solvable with derived length n , then the derived length of G is at most $m + n$.

We are now ready to complete our proof of the Schur-Zassenhaus theorem.

3.12. Theorem. *Let $N \triangleleft G$, where G is finite and $|N|$ and $|G : N|$ are coprime, and assume either that N is solvable or that G/N is solvable. Then all complements for N in G are conjugate.*

Proof. We proceed by induction on $|G|$. Let $U \subseteq G$ be arbitrary. We will show that U satisfies the hypotheses of the theorem with respect to its normal subgroup $U \cap N$, and also that if U contains a complement H for N in G , then H is also a complement for $U \cap N$ in U . It will then follow via the inductive hypothesis that if U is proper in G and contains two complements for N , these complements are conjugate in U and hence in G , as wanted.

Now $|U \cap N|$ divides $|N|$ and $|U : U \cap N| = |UN : N|$ divides $|G : N|$, and thus $|U \cap N|$ and $|U : U \cap N|$ are coprime. Also, either G/N is solvable, in which case $U/(U \cap N) \cong UN/N \subseteq G/N$ is solvable, or else N is solvable, and so $U \cap N$ is solvable. If U contains a complement H for N in G , then $|H|$ divides $|U|$ and is coprime to $|U \cap N|$, and hence $|H|$ divides $|U : U \cap N|$. But $|U : U \cap N|$ divides $|G : N| = |H|$, and so we have $|H| = |U : U \cap N|$,

and therefore H complements $U \cap N$ in U . This establishes the assertions of the previous paragraph.

Next, we consider factor groups. Suppose $L \triangleleft G$, and write $\overline{G} = G/L$, so that $\overline{N} \triangleleft \overline{G}$. Since \overline{N} is a homomorphic image of N , it is solvable if N is, and its order divides $|N|$. Also $\overline{G}/\overline{N} \cong G/NL$ is a homomorphic image of G/N , and so it is solvable if G/N is, and its order divides $|G : N|$. In other words, \overline{G} satisfies the hypotheses with respect to the normal subgroup \overline{N} . If H is a complement for N in G , then $|\overline{H}|$ is coprime to $|\overline{N}|$, and so $\overline{N} \cap \overline{H} = 1$. Also, $\overline{N}\overline{H} = \overline{NH} = \overline{G}$, and thus \overline{H} is a complement for \overline{N} in \overline{G} .

Let H and K be complements for N in G . If $L > 1$, then by the inductive hypothesis applied in \overline{G} , we deduce that \overline{H} and \overline{K} are conjugate in \overline{G} , and thus HL and KL are conjugate in G . We can thus write $HL = (KL)^g$ for some element $g \in G$, and hence HL contains both H and K^g , each of which is a complement for N in G . If $HL < G$, therefore, it follows by the result of the first paragraph of the proof that H and K^g are conjugate, and thus H and K are conjugate, as required. We can thus assume that $HL = G$ for every nonidentity normal subgroup L of G .

Suppose that N is solvable, and note that we can assume that $N > 1$, or else $H = G = K$ and there is nothing to prove. Let $L \subseteq N$ be a minimal normal subgroup of G , so that L is abelian by Lemma 3.11. By the result of the previous paragraph, $HL = G$, and since $L \subseteq N$ and $|N| = |G : H|$, it follows that $N = L$, and so N is abelian and we are done by Theorem 3.5.

Finally, assume that G/N is solvable. We can assume that $N < G$, or else $H = 1 = K$ and there is nothing to prove. Let M/N be minimal normal in G/N , and apply Lemma 3.11 to conclude that M/N is a p -group for some prime p . Also, since p divides $|G : N|$, we see that p does not divide $|N|$.

Since $NH = G$ and $N \subseteq M$, Dedekind's lemma yields $M = N(M \cap H)$, and it follows that $M \cap H$ complements N in M . In particular $|M \cap H| = |M : N|$, and so $M \cap H$ is a p -group. Also, $|M : M \cap H| = |N|$ is not divisible by p , and we conclude that $M \cap H$ is a Sylow p -subgroup of M . Similarly, $M \cap K$ is a Sylow p -subgroup of M , and thus by the Sylow C-Theorem, $M \cap H = (M \cap K)^m = M \cap K^m$ for some element $m \in M$.

Now write $L = M \cap H = M \cap K^m$, and note that $L \triangleleft H$ and $L \triangleleft K^m$ since $M \triangleleft G$. Thus H and K^m are complements for N in G that are contained in $\mathbf{N}_G(L)$. If $\mathbf{N}_G(L) < G$, we are done by the first part of the proof. We can assume, therefore, that $L \triangleleft G$, and since $L > 1$, we have $LH = G$. But $L \subseteq H$, and so $H = G$ and thus also $K = G$ and we are done in this case too. ■

Perhaps it is of interest to note that the conjugacy part of Theorem 3.5 was used in the proof of Theorem 3.12 only in the case where N is solvable. Conjugacy in the case where G/N is solvable ultimately depends on the conjugacy of Sylow subgroups, but not on Theorem 3.5.

Problems 3B

3B.1. Show that a maximal subgroup of a finite solvable group must have prime power index.

Hint. Look at a minimal normal subgroup and work by induction.

3B.2. Suppose $1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = G$, where the factors N_i/N_{i-1} are abelian for $1 \leq i \leq r$. Show that G is solvable. (Note that we are not assuming that the subgroups N_i are normal in G .)

3B.3. Let G be finite and let $1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = G$, where the factors N_i/N_{i-1} are simple for $1 \leq i \leq r$. Show that G is solvable if and only if these factors all have prime order.

Note. Recall that a subnormal series such as $\{N_i\}$, where the factors are simple, is a composition series for G , and note that if G is finite, such a series necessarily exists. Although G may have several different composition series, the Jordan-Hölder theorem asserts that the factors N_i/N_{i-1} are uniquely determined by G (except for the order in which they occur). This problem says that solvable finite groups are exactly the groups for which every composition factor has prime order.

3B.4. Let $N \triangleleft G$, where $|N|$ and $|G : N|$ are coprime. Let $U \subseteq G$, where $|U|$ divides $|G : N|$, and assume that either N or U is solvable. Show that U is contained in some complement H for N in G .

3B.5. Suppose that $P \in \text{Syl}_p(G)$ and that $P \subseteq \mathbf{Z}(G)$. Show that the set X of elements of G with order not divisible by p is a subgroup of G , and that $G = X \times P$.

3B.6. Let $N \triangleleft G$ and $g \in G$, and suppose that when Ng is viewed as an element of G/N , it has order m .

- (a) Show that there exists $h \in Ng$ such that every prime divisor of $o(h)$ divides m .
- (b) If m and $|N|$ are coprime, show that the element h of part (a) must have order m .
- (c) Now assume that Ng is conjugate to its inverse in G/N and that m and $|N|$ are coprime. Let $h \in Ng$ be as in (a). Show that h is conjugate to its inverse in G .

Hint. For (a), find a cyclic π -subgroup C such that $NC = N\langle q \rangle$, where π is the set of prime divisors of m . For (c), let $x \in G$, where $(Nq)^{Nx} = (Nq)^{-1}$. Observe that x normalizes $N\langle h \rangle$. Consider the subgroup $\langle h \rangle^x$.

3B.7. A group G is **supersolvable** if there exist normal subgroups N_i with

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = G,$$

and where each factor N_i/N_{i-1} is cyclic for $1 \leq i \leq r$. Clearly, supersolvable groups are solvable, and it is routine to check that subgroups and factor groups of supersolvable groups are supersolvable. Suppose now that G is finite and supersolvable.

- (a) Show that the order of every minimal normal subgroup of G is prime.
- (b) Show that the index of every maximal subgroup of G is prime.

Hint. For (b), look at a minimal normal subgroup and work by induction.

3B.8. Let G be finite, and assume that every maximal subgroup of G has prime index. Show that G is solvable. Show also that G has a normal Sylow p -subgroup, where p is the largest prime divisor of $|G|$, and that G has a normal q -complement, where q is the smallest prime divisor of $|G|$.

Note. In fact, G must be supersolvable, but this theorem of B. Huppert is much harder to prove. Recall that a **q -complement** in a group G is subgroup with q -power index and having order not divisible by q . In other words, it is a subgroup whose index is the order of a Sylow q -subgroup.

3B.9. Let G be finite and supersolvable. If n is a divisor of $|G|$, show that G has a subgroup of order n .

Hint. Look at a minimal normal subgroup and work by induction.

3B.10. Let G be finite and supersolvable, and suppose that p is the largest prime divisor of $|G|$. Show that G has a normal Sylow p -subgroup.

Hint. Look at a minimal normal subgroup and work by induction.

3B.11. As usual, let $\Phi(G)$ be the Frattini subgroup of the finite group G . Show that every prime divisor of $|\Phi(G)|$ also divides $|G : \Phi(G)|$.

3B.12. Let G be solvable, and assume that $\Phi(G) = 1$. Let M be a maximal subgroup of G , and suppose that $H \subseteq M$. Show that G has a subgroup with index equal to $|M : H|$.

3B.13. Show that every finite group contains a unique largest solvable normal subgroup.

3B.14. Let $F = \mathbf{F}(G)$, where G is finite, and let $C = \mathbf{C}_G(F)$. Show that $\mathbf{Z}(F)$ is the unique largest solvable normal subgroup of C .

Hint. Problem ID.19 is relevant.

Note. If G is solvable, it follows that $C = \mathbf{Z}(F)$. This shows that for solvable groups, $\mathbf{F}(G) \supseteq \mathbf{C}_G(\mathbf{F}(G))$.

3B.15. (Berkovich) Let G be solvable, and let $H < G$ be a proper subgroup having the smallest possible index in G . Show that $H \triangleleft G$.

3C

There exists an extensive and well developed theory of finite solvable groups to which we give only superficial mention here. (Readers interested in pursuing this might wish to consult the comprehensive book on solvable groups by Doerk and Hawkes.) Underlying this theory are some results of Philip Hall analogous to the Sylow E-, C- and D-theorems, but where sets of primes replace individual primes. Hall's results are not especially difficult to prove directly, but they also follow easily from the Schur-Zassenhaus theorem, and that is why we present them here.

Recall that if π is a set of primes, then a π -group is a finite group such that all primes dividing its order lie in π , and a π -subgroup of a group G is simply a subgroup that happens to be a π -group. A **Hall π -subgroup** of a finite group G is a π -subgroup with index involving no prime of π .

For convenience in discussing Hall's theorems and related topics, we say that an integer m is a π -number if every prime divisor of m lies in π . Also, we write π' to denote the complement of π in the set of all prime numbers, so that a π' -number is an integer with no divisors in π . (In the case where π consists of a single prime p , we generally write p' in place of $\{p\}'$.) A subgroup H of G , therefore, is a Hall π -subgroup of G precisely when $|H|$ is a π -number and $|G : H|$ is a π' -number, or equivalently, $|H|$ is the largest π -number dividing $|G|$.

Of course, if π consists of just one prime, so that $\pi = \{p\}$, then a Hall π -subgroup is just a Sylow p -subgroup, and we know by the Sylow E-theorem that such a subgroup actually exists for every finite group. But if $|\pi| > 1$, then an arbitrary finite group G can fail to have a Hall π -subgroup. The situation is different, however, if G is solvable.

3.13. Theorem (Hall-E). *Suppose that G is a finite solvable group, and let π be an arbitrary set of primes. Then G has a Hall π -subgroup.*

Proof. We can certainly assume that $G > 1$, and we proceed by induction on $|G|$. Let M be a minimal normal subgroup of G and let \overline{H} be a Hall π -subgroup of $\overline{G} = G/M$, where $H \supseteq M$. (Of course, \overline{H} exists by the inductive

hypothesis.) Then $|H : M| = |\overline{H}|$ is a π -number and $|G : H| = |\overline{G} : \overline{H}|$ is a π' -number.

By Theorem 3.11, we know that M is a p -group for some prime p . If $p \in \pi$, then since $|H| = |M||H : M|$, it follows that $|H|$ is a π -number, and thus H is a Hall π -subgroup of G , as wanted. If $p \notin \pi$, on the other hand, then $|M|$ and $|H : M|$ are coprime, and hence by the Schur-Zassenhaus theorem, M has a complement K in H . Then $|K| = |H : M|$ is a π -number and $|G : K| = |G : H||H : K| = |G : H||M|$ is a π' -number. In this case, K is the desired Hall π -subgroup of G . ■

We used the Schur-Zassenhaus theorem to prove Theorem 3.13, but nothing that deep is really needed. In fact, the Hall E-theorem can be proved using a fairly elementary argument.

Next, we present (with a somewhat sketchy proof) the Hall C-theorem, but we defer the Hall D-theorem to the problems at the end of this section.

3.14. Theorem (Hall-C). *Suppose that G is a finite solvable group, and let π be an arbitrary set of primes. Then all Hall π -subgroups of G are conjugate.*

Proof. As in the previous proof, we proceed by induction on $|G|$. Assuming that $G > 1$, choose a minimal normal subgroup M of G , which must be a p -group for some prime p . Let H and K be Hall π -subgroups of G , and observe that \overline{H} and \overline{K} are Hall π -subgroups of $\overline{G} = G/M$. By the inductive hypothesis, therefore, \overline{H} and \overline{K} are conjugate in \overline{G} , and it follows that HM and KM are conjugate in G . We can thus write $HM = (KM)^g$ for some element $g \in G$.

If $p \in \pi$, then $|HM|$ and $|KM|$ are π -numbers. But $|H| = |K|$ is the largest π -number dividing $|G|$, and it follows that $H = HM$ and $K = KM$, and so $H = K^g$, as wanted. If $p \notin \pi$, then H and K^g are complements in HM for the normal Hall subgroup M . The conjugacy part of the Schur-Zassenhaus theorem then yields the result. ■

One might wonder how essential solvability is in the Hall E-theorem. Certainly, some nonsolvable groups have Hall π -subgroups for some interesting sets π of primes. (By “interesting” here, we mean cases where π contains more than one, but not all of the prime divisors of the group order. In other cases, the existence of a Hall π -subgroup is either a triviality, or is guaranteed by Sylow’s theorem.) For example, the simple group A_5 contains the Hall $\{2, 3\}$ -subgroup A_4 , and the simple group of order 168 contains a Hall $\{3, 7\}$ -subgroup and a Hall $\{2, 3\}$ -subgroup.

We say that G satisfies E_π if it contains a Hall π -subgroup. We know that solvable groups satisfy E_π for all sets π of primes, and perhaps surprisingly,

the converse is true: if G satisfies E_π for all π , then G must be solvable. In fact, G is solvable if it satisfies E_π for all prime sets of the form $\pi = p'$, where p is an arbitrary prime. (Recall that p' is the complement of $\{p\}$ in the set of all primes.) A Hall p' -subgroup of G is called a p -complement in G , and of course, if $|G|$ is not divisible by p , then G is a p -complement of itself. The condition $E_{p'}$ has no content in this case, and so we can state the converse of the Hall E-theorem as follows.

3.15. Theorem. *Suppose that a finite group G has a p -complement for all prime divisors p of $|G|$. Then G is solvable.*

What does this converse of Hall's E-theorem say in the case where $|G|$ involves just two (or fewer) primes? If $|G| = p^a q^b$, where p and q are prime and a and b are nonnegative integers, then a Sylow q -subgroup of G is a p -complement and a Sylow p -subgroup of G is a q -complement. In this situation, Sylow's theorem guarantees that the hypotheses of Theorem 3.15 are satisfied, and thus the theorem says that every group of order $p^a q^b$ is solvable. This is Burnside's famous $p^a q^b$ -theorem, which we are certainly not prepared to prove at this point. (We present a proof in Chapter 7, however.) But if we are willing to assume Burnside's theorem, it is not hard to establish Theorem 3.15 in its full generality.

We need a few preliminary results. The first of these is fairly standard, and it also appears in the group-theory review in the appendix.

3.16. Lemma. *Let $H, K \subseteq G$, where G is a finite group, and suppose that $|G : H|$ and $|G : K|$ are coprime. Then $G = HK$ and $|H : H \cap K| = |G : K|$.*

Proof. Let $D = H \cap K$, and observe that since $|G : D| = |G : H||H : D|$, the index $|G : D|$ is divisible by $|G : H|$. Similarly, $|G : D|$ is divisible by $|G : K|$, and since we are assuming that $|G : H|$ and $|G : K|$ are coprime, we conclude that their product divides $|G : D|$. In particular, $|G : H||G : K| \leq |G : D|$, and hence $|G| \leq |H||K|/|D| = |HK|$. It follows that $HK = G$, as wanted. Also, since equality holds here, we obtain $|G : K| = |G|/|K| = |H|/|D| = |H : H \cap K|$, as wanted. ■

We mention that this proof of Lemma 3.16 is valid only if $|G|$ is finite, but in fact, the lemma is true even if G is infinite, assuming, of course, that H and K have finite coprime indices.

The following is due to H. Wielandt.

3.17. Theorem. *Let $H, K, L \subseteq G$, where G is a finite group, and suppose that the indices $|G : H|$, $|G : K|$ and $|G : L|$ are pairwise coprime. If each of H , K and L is solvable, then G is solvable.*

Proof. Since the result is trivial if $|G| = 1$, we can proceed by induction on $|G|$. Suppose that $N \triangleleft G$, and consider the subgroups \overline{H} , \overline{K} and \overline{L} of $\overline{G} = G/N$. Since these are homomorphic images of the solvable groups H , K and L , respectively, each of them is solvable. Also $|\overline{G} : \overline{H}| = |\overline{G} : \overline{NH}| = |G : NH|$, which divides $|G : H|$. Similarly, $|\overline{G} : \overline{K}|$ divides $|G : K|$ and $|\overline{G} : \overline{L}|$ divides $|G : L|$, and so the indices of \overline{H} , \overline{K} and \overline{L} are pairwise coprime. If $N > 1$, therefore, \overline{G} is solvable by the inductive hypothesis.

If $H = 1$, then $|G| = |G : H|$ is relatively prime to $|G : K|$, and thus $G = K$ is solvable. We can assume, therefore, that $H > 1$, and we choose a minimal normal subgroup M of H . By Lemma 3.11, we know that M is a p -group for some prime p , and since p cannot divide both $|G : K|$ and $|G : L|$, we can assume that p does not divide $|G : K|$. In other words, K contains a full Sylow p -subgroup of G , and by Sylow theory, some conjugate of that Sylow subgroup contains the p -subgroup M . Thus $M \subseteq K^g$ for some element $g \in G$.

Now $|G : K^g| = |G : K|$ is relatively prime to $|G : H|$, and hence by Lemma 3.16, we have $G = HK^g$. Let $x \in G$ be arbitrary, and write $x = uv$, where $u \in H$ and $v \in K^g$. Then $M^x = M^{uv} = M^v \subseteq K^g$, where the second equality holds because $u \in H$ and $M \triangleleft H$. All conjugates of M , therefore, lie in K^g , and hence the subgroup M^G that they generate is contained in K^g , which is solvable. Then M^G is a nonidentity solvable normal subgroup of G , and also, G/M^G is solvable by the first paragraph of the proof. It follows by Lemma 3.10(e) that G is solvable, as required. ■

Proof of Theorem 3.15 (assuming Burnside). We proceed by induction on the number n of different primes that divide $|G|$. If $n = 1$, then G is a p -group, and hence is solvable, and if $n = 2$, then G is solvable by Burnside's theorem. We can assume, therefore, that at least three primes p , q and r divide $|G|$, and we choose a p -complement H , a q -complement K and an r -complement L in G . The indices of these subgroups are respectively, a power of p , a power of q and a power of r , and so they are pairwise coprime. If we can show that H , K and L are solvable, it will follow by Theorem 3.17 that G is solvable, and we will be done.

The prime divisors of $|H|$ are just the prime divisors of $|G|$ other than p , and so there are exactly $n - 1$ of them. Let s be one of these prime divisors of $|H|$, and let Q be an s -complement in G . Then $|G : H|$ is a power of p and $|G : Q|$ is a power of s , and so these indices are coprime, and it follows by Lemma 3.16 that $|H : H \cap Q| = |G : Q|$, which is the full power of s dividing $|G|$. Since this is also the full power of s dividing $|H|$, it follows that $H \cap Q$ is an s -complement in H . This shows that H has an s -complement for each of the $n - 1$ primes s dividing its order, and so H is solvable by the inductive hypothesis. Similarly, K and L are solvable, and the proof is complete. ■

We have seen that for every nonsolvable finite group G , there is a prime set π for which G fails to have a Hall π -subgroup. How about conjugacy? Since Hall π -subgroups do sometimes exist in nonsolvable groups, we can ask whether or not (for a fixed prime set π) all Hall π -subgroups of a nonsolvable group G must be conjugate. The answer is “no”; they need not even be isomorphic. In the simple group $PSL(2, 11)$ of order $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$, for example, there exists a Hall $\{2, 3\}$ -subgroup isomorphic to the alternating group A_4 , and there is another Hall $\{2, 3\}$ -subgroup isomorphic to the dihedral group D_{12} . These groups of order 12 are certainly not isomorphic. We close this discussion by mentioning (without proof) a lovely theorem of Wielandt which asserts that if G has a *nilpotent* Hall π -subgroup, then all Hall π -subgroups of G are conjugate.

Problems 3C

3C.1. Let $U \subseteq G$ be a π -subgroup, where π is a set of primes and G is solvable and finite. Show that U is contained in some Hall π -subgroup of G .

Hint. Use Problem 3B.4.

Note. This, of course, is the Hall D-theorem.

3C.2. Let π be a set of primes, and suppose that G has a p -complement H_p for each prime $p \in \pi$. Show that $\bigcap_{p \in \pi} H_p$ is a Hall π' -subgroup of G .

3C.3. A **Sylow system** in a group G is a set \mathcal{S} of Sylow subgroups of G , one chosen from $\text{Syl}_p(G)$ for each prime divisor p of $|G|$, and such that $PQ = QP$ for all $P, Q \in \mathcal{S}$.

- (a) Show that if G has a Sylow system, then it has a Hall π -subgroup for every set π of primes.
- (b) If G is solvable, prove that it has a Sylow system.

Hint. For (b), choose a p -complement H_p of G for each prime divisor of $|G|$, and consider intersections of all but one of these p -complements.

3C.4. Let M be minimal normal in a finite solvable group G , and assume that $M = \mathbf{C}_G(M)$. Show that G splits over M and that all complements for M in G are conjugate.

Hint. Let L/M be minimal normal in G/M , and note that L/M is a q -group for some prime q . Show that q does not divide $|M|$, and consider a Sylow q subgroup of L .

3C.5. Let H be a maximal subgroup of G , where G is solvable, and assume that $\text{core}_G(H) = 1$. Show that G has a unique minimal normal subgroup M , that H complements M and that $M = \mathbf{C}_G(M)$. Deduce that if K is also maximal in G with trivial core, then H and K are conjugate in G .

3C.6. Let G be finite and solvable, and suppose that $x, y, z \in G$ have orders that are pairwise relatively prime. If $xyz = 1$, show that $x = 1$, $y = 1$ and $z = 1$.

Hint. Work by induction on the derived length of G .

3C.7. A **Carter subgroup** of a solvable group G is a nilpotent subgroup C such that $C = \mathbf{N}_G(C)$.

- (a) Show that every solvable group has a Carter subgroup.
- (b) Show that all Carter subgroups of the solvable group G are conjugate in G .
- (c) If C is a Carter subgroup of G and G/N is nilpotent for some normal subgroup N of G , show that $NC = G$.

Note. This problem and the next one seem quite a bit harder than most of the problems in this book. We present them as challenges to the reader, and to give a taste of some of the theory of solvable groups that we have omitted.

3C.8. Let G be solvable. A **nilpotent injector** of G is a nilpotent subgroup I containing the Fitting subgroup $\mathbf{F}(G)$, and maximal with this property. Prove that all nilpotent injectors of G are conjugate in G .

3D

A finite group G is said to be **π -separable**, where π is some set of primes, if there exists a normal series

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_r = G$$

such that each factor N_i/N_{i-1} is either a π -group or a π' -group. (Observe that a π -separable group is the same thing as a π' -separable group.) It is easy to prove, as we shall see, that finite solvable groups are π -separable for all prime sets π , and so π -separability can be viewed as a generalization of solvability.

First, we mention that if G is π -separable, then so too is every subgroup and every homomorphic image. (This fact is easy to establish, and we trust that the reader can supply a proof.) Next, we recall that $\mathbf{O}_\pi(G)$ is the unique largest normal π -subgroup in G , which may, of course, be the trivial subgroup. (The uniqueness is an immediate consequence of the fact that if N

and M are normal π -subgroups of G , then NM is also a normal π -subgroup.) Because $\mathbf{O}_\pi(G)$ is uniquely determined, it is, of course, characteristic in G .

In the definition of π -separability, we can renumber the normal subgroups N_i if necessary, in order to eliminate repeats among them. If G is π -separable and nontrivial, therefore, we can assume that $N_1 > 1$. Since N_1 is either a normal π -subgroup or a normal π' -subgroup of G , we see that either $\mathbf{O}_\pi(G) > 1$ or $\mathbf{O}_{\pi'}(G) > 1$ (or both). In particular, G has a nontrivial characteristic subgroup N that is either a π -group or a π' -group. Also, if $N < G$, then G/N is π -separable, and so we can find a nontrivial characteristic subgroup M/N of G/N that is either a π -group or a π' -group. Continuing like this, we can construct a series of characteristic subgroups of G whose factors are π -groups and π' -groups.

The discussion in the previous paragraph shows that if we strengthen the condition on the normal subgroups N_i in the definition of π -separability, and we require them to be characteristic, and not merely normal, then the same class of groups would result. Somewhat paradoxically, this observation allows us to prove that a *weakened* version of the definition also yields exactly the same class of groups. It suffices to consider subnormal series.

3.18. Lemma. *Suppose that G is a finite group and that*

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = G$$

is a series of subgroups such that each factor N_i/N_{i-1} is either a π -group or a π' -group. Then G is π -separable.

Proof. We can assume that $r > 0$, and we proceed by induction on r . Since N_{r-1} is π -separable by the inductive hypothesis, the preceding remarks guarantee that there exists a characteristic series

$$1 = M_0 \subseteq \cdots \subseteq M_s = N_{r-1}$$

having π and π' -factors. Since $N_{r-1} \triangleleft G$, the characteristic subgroups M_i of N_{r-1} are normal in G , and hence G has the normal series

$$1 = M_0 \subseteq \cdots \subseteq M_s = N_{r-1} \subseteq N_r = G$$

with π and π' -factors. Thus G is π -separable, as desired. ■

3.19. Corollary. *Let G be finite and solvable. Then G is π -separable for every set π of primes.*

Proof. Consider a composition series for G . (Recall that this is a chain of subgroups

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = G$$

such that each of the factors N_i/N_{i-1} is simple.) Since we are assuming that G is solvable, its composition factors are solvable too, and thus each of

the simple groups N_i/N_{i-1} has prime order. But every prime p is either a π -number or a π' -number, depending on whether $p \in \pi$ or $p \notin \pi$, and thus G is π -separable by Lemma 3.18. ■

A somewhat stronger condition than “ π -separability” is “ π -solvability”. A finite group G is π -solvable if it has a normal series where each factor is either a π' -group or is a solvable π -group. (Of course, a solvable group is automatically π -solvable for every set π of primes.) We shall not have much to say about π -solvable groups except in the case where $\pi = \{p\}$ consists of a single prime. Since p -groups are solvable, it follows that $\{p\}$ -separability and $\{p\}$ -solvability are the same thing, and groups in this class are generally described as being “ p -solvable”. Note that a finite group is solvable if and only if it is p -solvable for every prime p .

A key result about π -separable groups is the following, which is a generalization of Hall’s E-theorem, with essentially the same proof.

3.20. Theorem. *Let G be a π -separable group. Then G has a Hall π -subgroup.*

Proof. We proceed by induction on $|G|$. Suppose first that $\mathbf{O}_\pi(G) > 1$. By the inductive hypothesis, the group $G/\mathbf{O}_\pi(G)$ has a Hall π -subgroup $H/\mathbf{O}_\pi(G)$, and it is immediate that H is a Hall π -subgroup of G . If $\mathbf{O}_\pi(G) = 1$, then since we can certainly assume that G is nontrivial, we have $\mathbf{O}_{\pi'}(G) > 1$. We can thus apply the inductive hypothesis to $G/\mathbf{O}_{\pi'}(G)$ to produce a Hall π -subgroup $H/\mathbf{O}_{\pi'}(G)$. By the Schur-Zassenhaus theorem, $\mathbf{O}_{\pi'}(G)$ has a complement in H , and it is easy to see that such a complement is the desired Hall π -subgroup of G . ■

The reader might guess that analogs of the C-theorem and D-theorem also hold in the context of π -separable groups, and indeed they do. Their proofs rely on the conjugacy part of the Schur-Zassenhaus theorem, however, and thus they require either some solvability assumption or else an appeal to the Feit-Thompson theorem.

Some of the basic definitions and results about π -separability go back to the work of S. A. Cunihin in 1948, but it was the historic paper of Philip Hall and Graham Higman in 1956 that established a number of deeper properties, at least for p -solvable groups. A basic and frequently used result in the Hall-Higman paper is their Lemma 1.2.3, which we state here somewhat more generally: for π -separable groups.

3.21. Theorem (Hall-Higman 1.2.3). *Let G be a π -separable group, and assume that $\mathbf{O}_{\pi'}(G) = 1$. Then $\mathbf{O}_\pi(G) \supseteq \mathbf{C}_G(\mathbf{O}_\pi(G))$.*

Proof. Write $C = \mathbf{C}_G(\mathbf{O}_\pi(G))$ and let $B = C \cap \mathbf{O}_\pi(G)$. Our goal is to show that $B = C$, and so we assume that $B < C$, and we work to derive a contradiction. Note that B and C are normal (and in fact, characteristic) in G and that B is a π -group.

Since C/B is a nontrivial π -separable group, it has a nontrivial characteristic subgroup K/B , where K/B is either a π -group or a π' -group. Also, since K/B is characteristic in $C/B \triangleleft G/B$, we see that $K/B \triangleleft G/B$, and hence $K \triangleleft G$. Since B is a π -group, it follows that if K/B is also a π -group, then K is a normal π -subgroup of G , and hence $K \subseteq \mathbf{O}_\pi(G)$. This is not the case, however, since $B < K \subseteq G$ and $B = C \cap \mathbf{O}_\pi(G)$. We can thus conclude that K/B is a π' -group. By the Schur-Zassenhaus theorem, therefore, there is a complement H for B in K , and we see that $H > 1$.

We have $H \subseteq G = \mathbf{C}_G(\mathbf{O}_\pi(G)) \subseteq \mathbf{C}_G(B)$, where the final containment holds because $B \subseteq \mathbf{O}_\pi(G)$. Thus B centralizes H and since $BH = K$, we see that $H \triangleleft K$. Thus $1 < H \subseteq \mathbf{O}_{\pi'}(K) \triangleleft G$, and this is a contradiction since by hypothesis, $\mathbf{O}_{\pi'}(G) = 1$, and hence G has no nontrivial normal π' -subgroup. ■

In a group G , a normal subgroup N that contains its own centralizer can be thought of as a “large” subgroup, and indeed, in this situation, the index $|G : N|$, is bounded in terms of N . To see this, recall that for an arbitrary normal subgroup N , the factor group $G/\mathbf{C}_G(N)$ is isomorphically embedded in $\text{Aut}(N)$, and so $|G : \mathbf{C}_G(N)| \leq |\text{Aut}(N)|$. If $\mathbf{C}_G(N) \subseteq N$, therefore, we have $|G : N| \leq |\text{Aut}(N)|$. Lemma 1.2.3 asserts that in a π -separable group G for which $\mathbf{O}_{\pi'}(G) = 1$, the normal subgroup $\mathbf{O}_\pi(G)$ is large in this sense. Another example of a characteristic subgroup that is guaranteed to be “large” is the Fitting subgroup $\mathbf{F}(G)$ of a solvable group G . (See Problem 3B.14 and the note following it.) In Chapter 9, we discuss the “generalized Fitting subgroup” $\mathbf{F}^*(G)$, which always contains its own centralizer, with no extra assumption on G .

We close this section by showing how the Hall-Higman Lemma 1.2.3 can be used. First, we need a definition. If G is π -separable, the π -length of G is the minimum possible number of factors that are π -groups in any normal series for G in which each factor is either a π -group or a π' -group. For example, G has π -length 1 precisely when G is not a π' -group and there exist normal subgroups $N \subseteq M$ of G such that N and G/M are π' -groups and M/N is a π -group.

3.22. Theorem. *Let G be a π -separable group, and suppose that a Hall π -subgroup of G is abelian. Then the π -length of G is at most 1.*

Proof. Consider the π -separable group $\overline{G} = G/\mathbf{O}_{\pi'}(G)$, and observe that $\mathbf{O}_{\pi'}(\overline{G}) = 1$. Let H be an abelian Hall π -subgroup of G , and note that

\overline{H} is a Hall π -subgroup of \overline{G} . Then \overline{H} contains every normal π -subgroup of \overline{G} , and in particular, $\mathbf{O}_\pi(\overline{G}) \subseteq \overline{H}$. But \overline{H} is abelian, and thus $\overline{H} \subseteq \mathbf{C}_{\overline{G}}(\mathbf{O}_\pi(\overline{G})) \subseteq \mathbf{O}_\pi(\overline{G})$, where the last containment follows by the Hall-Higman Lemma 1.2.3. Thus $\overline{H} = \mathbf{O}_\pi(\overline{G})$, and we have $\overline{H} \triangleleft \overline{G}$. Thus $1 \subseteq N \subseteq NH \subseteq G$ is a normal series for G with just one π -factor, and the proof is complete. ■

Problems 3D

3D.1. Let G be a p -solvable group, and let $P \in \text{Syl}_p(G)$.

(a) If $\mathbf{O}_{p'}(G) = 1$, show that $\mathbf{Z}(P) \subseteq \mathbf{O}_p(G)$.

(b) Show that the p -length of G is at most the nilpotence class of P .

3D.2. Let $Z \subseteq \mathbf{Z}(G)$ and write $\overline{G} = G/Z$. Show that $\mathbf{O}_\pi(\overline{G}) = \overline{\mathbf{O}_\pi(G)}$ for every set π of primes.

3D.3. Let G be π -separable, and assume that $\mathbf{O}_\pi(G)\mathbf{O}_{\pi'}(G) \subseteq \mathbf{Z}(G)$. Show that G is abelian.

3D.4. Let H act by automorphisms on G , and assume that $|H|$ and $|\Phi(G)|$ are coprime. Suppose that the induced action of H on $G/\Phi(G)$ is trivial, which means that each coset of $\Phi(G)$ in G is setwise invariant under H . Show that the action of H on G is trivial.

Hint. It is no loss to assume that H is a q -group for some prime q . Consider the decomposition of each coset of $\Phi(G)$ into H -orbits.

3D.5. Let G be p -solvable, and let $P \in \text{Syl}_p(G)$. Suppose that $P \subseteq \mathbf{N}_G(K)$, where $K \subseteq G$ is a subgroup of order not divisible by p . Show that $K \subseteq \mathbf{O}_{p'}(G)$.

Hint. First, consider the case where $\mathbf{O}_{p'}(G) = 1$. To do the general case, consider the group $\overline{G} = G/\mathbf{O}_{p'}(G)$.

3E

Let A be a group that acts via automorphisms on some group G . By definition, A permutes the elements of G , but because we have an action by automorphisms, A also permutes many other kinds of group-theoretic objects associated with G . For example, A acts on the set of all Sylow p -subgroups of G for any given prime p , and A acts on the set of all conjugacy classes of G . It is of interest to find, or at least to prove the existence of, A -invariant objects of various kinds. Once one has found an A -invariant object, there are usually further actions that can be studied. For example, if H is an

A -invariant subgroup of G , then A acts on the set of right cosets or of left cosets of H in G , and on the set of conjugacy classes of H .

Of course, the most basic type of A -invariant object in G is an A -invariant *element*. These A -fixed points in G clearly form a subgroup, which is denoted $\mathbf{C}_G(A)$. To see why this centralizer notation is really quite natural, embed A and G in their semidirect product $\Gamma = G \rtimes A$. We know that the original action of A on G is realized by conjugation within Γ , and thus $g^a = g$ if and only if g and a commute in Γ . Thus the A -fixed-point subgroup of G is exactly the centralizer of A in G , and this explains the notation $\mathbf{C}_G(A)$, which is used to denote the fixed-point subgroup even if the semidirect product has not been mentioned. Similarly, working in the semidirect product, we see that $\mathbf{C}_A(G)$ is the set of elements of A that act trivially on G , or in other words, it is the kernel of the action of A on G . This notation also can be used without mentioning the semidirect product.

It is especially easy to find A -invariant objects in G if A and G have co-prime orders, and this is the situation we study in this section. For example, we will prove the following.

3.23. Theorem. *Let A act via automorphisms on G , where A and G are finite groups, and suppose that $(|A|, |G|) = 1$. Assume also that at least one of A or G is solvable. Then for each prime p , the following hold.*

- (a) *There exists an A -invariant Sylow p -subgroup of G .*
- (b) *If S and T are A -invariant Sylow p -subgroups of G , then $S^c = T$ for some element $c \in \mathbf{C}_G(A)$.*

Note that Theorem 3.23(a) is a generalization of the Sylow E-theorem, to which it reduces when A is the trivial group, and similarly, 3.23(b) is a generalization of the Sylow C-theorem. Another way to think about this result is to imagine that we have a pair of magic eyeglasses through which only A -invariant objects can be seen. Theorem 3.23(a) asserts that even when we look at G through these A -glasses, the Sylow E-theorem can be seen to hold: there exists a *visible* Sylow p -subgroup for each prime p .

The Sylow C-theorem also remains true when G is viewed through the magic A -glasses. What the usual C-theorem says, of course, is that given two Sylow p -subgroups of G , say S and T , we can find an element $g \in G$ such that $S^g = T$. Now suppose that S and T are Sylow p -subgroups that we can see after donning our glasses. (In other words, they are A -invariant.) The glasses version of the Sylow C-theorem says that we can *see* an element g of G such that $S^g = T$. The assertion, in other words, is that S and T are conjugate by some A -invariant element: an element of the fixed-point subgroup $\mathbf{C}_G(A)$. (This, of course, is exactly the assertion

of Theorem 3.23(b).) We will also prove the glasses version of the Sylow D-theorem: if P is a visible (A -invariant) p -subgroup of G , then P is contained in some visible (A -invariant) Sylow p -subgroup.

How can the glasses version of the Sylow E-theorem and similar results be proved? In the case where A is a g -group for some prime q , an easy counting argument suffices, as follows. First, observe that we can assume that A is nontrivial, and thus q divides $|A|$, and so q does not divide $|G|$. Since $|\text{Syl}_p(G)|$ divides $|G|$, it follows that q does not divide $|\text{Syl}_p(G)|$. Now A acts on $\text{Syl}_p(G)$, and hence this set decomposes into A -orbits, at least one of which must have size not divisible by q . But we are assuming that A is a g -group, and so all A -orbits have g -power size. There must be an orbit of size 1, therefore, which means that the set $\text{Syl}_p(G)$ contains an A -invariant member, as required.

A similar (but slightly more technical) argument can be used to prove 3.23(b) in the case where A is a g -group, but it appears to be utterly impossible to make a counting argument like this work if $|A|$ is not a prime power. The following result of G. Glauberman provides an effective substitute, however. Unfortunately, the proof of Glauberman's lemma relies on the conjugacy part of the Schur-Zassenhaus theorem, and thus we must either appeal to the Feit-Thompson theorem, or else assume that something is solvable. (The solvability assumptions that appear in the statements of Theorem 3.23 and other results about coprime actions are not really necessary, of course, since at least one of $|A|$ or $|G|$ is odd, and hence by the Feit-Thompson theorem, at least one of A or G must be solvable.)

3.24. Lemma (Glauberman). *Let A act via automorphisms on G , where A and G are finite groups, and suppose that $(|A|, |G|) = 1$. Assume also that at least one of A or G is solvable. Suppose that A and G each act on some nonempty set Ω , where the action of G is transitive. Finally, assume the compatibility condition:*

$$(*) \quad (\alpha \cdot g) \cdot a = (\alpha \cdot a) \cdot g^a$$

for all $\alpha \in \Omega$, $a \in A$ and $g \in G$. The following then hold.

- (a) *There exists an A -invariant element $\alpha \in \Omega$.*
- (b) *If $\alpha, \beta \in \Omega$ are A -invariant, then there exists $c \in \mathbf{C}_G(A)$ such that $\alpha \cdot c = \beta$.*

Before proceeding with the proof of Glauberman's lemma, we show how it can be used to prove Theorem 3.23.

Proof of Theorem 3.23. The set $\text{Syl}_p(G)$ is nonempty by the Sylow E-theorem. Each of G and A act on $\text{Syl}_p(G)$, where G acts by conjugation and the action of A is induced by the given action of A on G . (Since each

element of A induces an automorphism of G , it carries Sylow p -subgroups of G to Sylow p -subgroups.) Also, by the Sylow C-theorem, the action of G on $\text{Syl}_p(G)$ is transitive. Once we check the compatibility condition of Glauberman's lemma, it will follow by 3.24(a) that $\text{Syl}_p(G)$ contains an A -invariant member, thereby establishing (a). We need to check that

$$(S^g)^a = (S^a)^{g^a}$$

for $S \in \text{Syl}_p(G)$, $a \in A$ and $g \in G$. (Recall that here, exponentiation by g means conjugation by g in G , but exponentiation by a denotes the given action of a .) Since A acts by automorphisms, however, we have

$$(S^g)^a = (g^{-1}Sg)^a = (g^a)^{-1}S^a g^a = (S^a)^{g^a},$$

as required. Assertion (b) is immediate from 3.24(b). ■

In the previous proof, it was trivial to check the compatibility condition of Glauberman's lemma. Indeed, it seems to be equally trivial to check it in virtually every application of 3.24.

Proof of Lemma 3.24. To prove (a), let $\Gamma = G \rtimes A$ be the semidirect product with respect to the given action of A on G , and as usual, identify A and G with appropriate subgroups of Γ . Every element of Γ is uniquely of the form ag , where $a \in A$ and $g \in G$, and so we can unambiguously define an action of Γ on Ω by setting $\alpha \cdot (ag) = (\alpha \cdot a) \cdot g$. To verify that this really is an action, let $a, b \in A$ and $g, h \in G$. Then for $\alpha \in \Omega$, we have

$$\begin{aligned} (\alpha \cdot (ag)) \cdot (bh) &= (((\alpha \cdot a) \cdot g) \cdot b) \cdot h = (((\alpha \cdot a) \cdot b) \cdot g^b) \cdot h \\ &= \alpha \cdot ((ab)(g^b h)) \\ &= \alpha \cdot ((ag)(bh)), \end{aligned}$$

as wanted, where the second equality holds because of the compatibility condition, which we are assuming.

Now fix $\alpha \in \Omega$ and let $U = \Gamma_\alpha$, the stabilizer of α in Γ . If $x \in \Gamma$, then since by assumption, G is transitive on Ω , we can write $\alpha \cdot x = \alpha \cdot g$ for some element $g \in G$, and thus $xg^{-1} \in U$. It follows that $x \in UG$, and so $UG = \Gamma$. Now $G \triangleleft \Gamma$, and hence $U \cap G \triangleleft U$. Also,

$$|U : U \cap G| = |UG : G| = |\Gamma : G| = |A|$$

is coprime to $|U \cap G|$, and thus the Schur-Zassenhaus theorem applies in U with respect to the normal subgroup $U \cap G$. Let H be a complement for $U \cap G$ in U , and note that $|H| = |U : U \cap G| = |A|$, and thus H is a complement for G in Γ . Since A is also a complement for G in Γ , the conjugacy part of the Schur-Zassenhaus theorem allows us to write $A = H^x$ for some element $x \in \Gamma$. But $H \subseteq U$, and so H stabilizes α . Then $A = H^x$

stabilizes $\alpha \cdot x$, and thus $\alpha \cdot x$ is an A -invariant member of Ω . This completes the proof of (a).

To prove (b), let α and β be A -invariant members of Ω . Since G is transitive on Ω , the set $X = \{g \in G \mid \alpha \cdot g = \beta\}$ is nonempty, and we need to find an A -invariant element in X . For this purpose, we propose to use part (a) of the lemma, with the set X in place of Ω . If $x \in X$, then $\alpha \cdot x = \beta$, and so for $a \in A$, we have

$$\alpha \cdot x^a = (\alpha \cdot a) \cdot x^a = (\alpha \cdot x) \cdot a = \beta \cdot a = \beta,$$

where the first and last equalities hold because α and β are A -invariant, and the second is a consequence of the compatibility condition. Thus $x^a \in X$, and so the action of A on G maps X into (and hence onto) itself, and we have an action of A on X .

Now let $H = G_\beta$, the stabilizer of β in G . If we apply the above argument with β in place of α and H in place of X , we conclude that the action of A on G maps H to itself, and this defines an action via automorphisms of A on H . Also, since H is a subgroup of G , we see that $(|A|, |H|) = 1$ and that at least one of A or H is solvable.

Now A acts on H and on X , and we show next that H acts transitively on X by right multiplication. If $x \in X$ and $h \in H$, then

$$\alpha \cdot (xh) = (\alpha \cdot x) \cdot h = \beta \cdot h = \beta,$$

and thus $xh \in X$ and H acts on X by right multiplication, as wanted. In fact, this action is transitive, since if $x, y \in X$, then $x^{-1}y$ fixes β , and so $x^{-1}y \in H$, and right multiplication by $x^{-1}y$ carries x to y .

At this point we know that A acts via automorphisms on the group H , that $(|A|, |H|) = 1$, and that at least one of A or H is solvable. Also, each of A and H acts on the nonempty set X , and the action of H on X is transitive, and thus we have almost everything we need to apply part (a) of the lemma to conclude that X contains an A -invariant element. What remains is to check the compatibility condition. What we need, in other words, is $(xh)^a = x^a h^a$ for $x \in X$, $h \in H$ and $a \in A$. This is obvious, however, since A acts on G via automorphisms, and thus X contains an A -invariant element, as required. ■

The magic-eyeglasses version of the Sylow D-theorem follows easily from Theorem 3.23(a); its proof does not require a direct appeal to Glauberman's lemma.

3.25. Corollary. *Let A act via automorphisms on G , where A and G are finite groups, and suppose that $(|A|, |G|) = 1$. Assume also that at least one of A or G is solvable. Let $P \subseteq G$ be an A -invariant p -subgroup for some prime p . Then P is contained in some A -invariant Sylow p -subgroup of G .*

Proof. Replacing P by a subgroup containing it if necessary, we can assume that P is not contained in any strictly larger A -invariant p -subgroup of G , and we show that in this case, $P \in \text{Syl}_p(G)$. Let $N = \mathbf{N}_G(P)$, and observe that N is A -invariant since it is uniquely determined by the A -invariant subgroup P . By Theorem 3.23(a), we can choose an A -invariant member $S \in \text{Syl}_p(N)$, and we observe that since P is a normal p -subgroup of N , it must be contained in the Sylow p -subgroup S . By our assumption, however, P cannot be properly contained in S since S is A -invariant, and thus $P = S$. Thus P is a Sylow p -subgroup of its normalizer N , and it follows that P is a Sylow p -subgroup of G . (To see this, let $P \subseteq Q \in \text{Syl}_p(G)$, and suppose that $P < Q$. Then since normalizers grow in p -groups, $Q \cap N$ is a p -subgroup of N strictly larger than the Sylow p -subgroup P , and this is impossible.) ■

Next, we consider conjugacy classes. In general, if K is a class of G and $H \subseteq G$ is a subgroup, then $K \cap H$ may be empty, and even if it is nonempty, all we can say is that $K \cap H$ is a union of classes of H . Usually, $K \cap H$ is not a single class of H . (Distinct classes of a subgroup H that are contained in the same class of G are said to be **fused** in G .) The situation is under much tighter control if the subgroup is the set of fixed points of a coprime action. In particular, there is no fusion in that case.

3.26. Theorem. *Let A act via automorphisms on G , where A and G are finite groups, and write $C = \mathbf{C}_G(A)$. Suppose that $(|A|, |G|) = 1$, and assume that at least one of A or G is solvable. Then the map $K \mapsto K \cap C$ defines a bijection from the set of A -invariant conjugacy classes of G onto the set of all conjugacy classes of C .*

Proof. Let K be an A -invariant class of G . Then A acts on K , and G acts transitively on K by conjugation. The compatibility condition of Glauberman's lemma is that $(x^g)^a = (x^a)^{g^a}$ for elements $x \in K$, $a \in A$ and $g \in G$, and as usual, it is trivial to see that this holds. By 3.24(a), therefore, K contains an A -invariant element, and thus $K \cap C$ is nonempty. Also, by 3.24(b), all elements of $K \cap C$ are conjugate in C , and thus $K \cap C$ is a class of C .

We now have the map $K \mapsto K \cap C$ from the set of A -invariant classes of G to the set of classes of C ; we must show that it is a bijection. If K and L are A -invariant classes of G , with $K \cap C = L \cap C$, then since $K \cap C$ is nonempty and is contained in both K and L , it follows that $K \cap L$ is nonempty, and thus $K = L$. Our map, therefore, is injective. For surjectivity, it is enough to show that every element of C lies in $K \cap C$ for some A -invariant class K of G . Of course, each element $c \in C$ lies in a unique class K of G , and so it suffices to show that K is A -invariant. If $a \in A$, then K^a is a class of G , and since $c^a = c$, we see that $c \in K \cap K^a$. Thus the classes K and K^a are

not disjoint, and we conclude that $K = K^a$, and hence K is A -invariant, as wanted. ■

Now we consider cosets. If A acts on G and $H \subseteq G$ is A -invariant, then as we observed previously, A permutes the left cosets of H in G and also the right cosets of H in G . In the case of a coprime action, we can determine which left cosets and which right cosets of H are A -invariant.

3.27. Theorem. *Let A act via automorphisms on G , where A and G are finite groups, and write $C = \mathbf{C}_G(A)$. Let $H \subseteq G$ be A -invariant subgroup, and suppose that $(|A|, |H|) = 1$ and that one of A or H is solvable. Then the A -invariant left cosets of H in G and the A -invariant right cosets of H in G are exactly those cosets of H that contain elements of C .*

Proof. If $a \in A$ and $c \in C$, then $(Hc)^a = H^a c^a = He$, and similarly, $(cH)^a = cH$, and so cosets of H that contain elements of C are A -invariant. Now suppose that X is an A -invariant left coset of H . Then H acts transitively by right multiplication on X and, of course, A acts on X and A acts via automorphisms on H . The compatibility condition for Glauberman's lemma in this situation is $(xh)^a = x^a h^a$ for $x \in X$, $h \in H$ and $a \in A$, and this holds since the given action of A on G is an action via automorphisms. By 3.24(a), therefore, X contains an element of C , as wanted.

To handle the right cosets, it suffices to observe that every right coset of H in G has the form $X^{-1} = \{x^{-1} \mid x \in X\}$ for some left coset X of H in G . Since X is A -invariant if and only if X^{-1} is, the desired result for right cosets is a consequence of that for left cosets. (Alternatively, if Y is a right coset of H in G , then $y \cdot h = h^{-1}y$ defines a transitive action of H on Y , and we can apply Glauberman's lemma directly.) ■

Actions on cosets are especially interesting for normal subgroups. Let A act on G via automorphisms, and suppose that $N \triangleleft G$ is A -invariant. Of course, the cosets of N in G are the elements of the factor group G/N , and since these are permuted by A , we see that A acts on G/N . In fact, this is an action via automorphisms since

$$(NxNy)^a = (Nxy)^a = Nx^a y^a = Nx^a Ny^a = (Nx)^a (Ny)^a.$$

The A -invariant cosets of N in G , therefore, are exactly the elements of the fixed-point subgroup $\mathbf{C}_{G/N}(A)$. We can use the bar convention to give a clean restatement of Theorem 3.27 in this situation, a statement that can be paraphrased as “fixed points come from fixed points (in coprime actions)”.

3.28. Corollary. *Let A act via automorphisms on G , where A and G are finite groups, and let $N \triangleleft G$ be A -invariant. Assume that $(|A|, |N|) = 1$ and*

that at least one of A or N is solvable. Writing $\overline{G} = G/N$, we have

$$\mathbf{C}_{\overline{G}}(A) = \overline{\mathbf{C}_G(A)}.$$

Proof. The A -fixed elements of \overline{G} are exactly the A -invariant cosets of N , which by 3.27 are exactly the cosets of N that contain elements of $C = \mathbf{C}_G(A)$. But the cosets of N that contain elements of C form the image \overline{C} of C in \overline{G} . ■

3.29. Corollary. *Let A act via automorphisms on G , where A and G are finite groups, and assume that $(|A|, |G|) = 1$. If the induced action of A on the Frattini factor group $G/\Phi(G)$ is trivial, then the action of A on G is trivial.*

Proof. We must show that each element $a \in A$ lies in $\mathbf{C}_A(G)$, and so it is no loss to assume that $A = \langle a \rangle$. Since A is cyclic, it is certainly solvable, and thus Corollary 3.28 applies with $\overline{G} = G/\Phi(G)$. Writing $C = \mathbf{C}_G(A)$, we have

$$\overline{G} = \mathbf{C}_{\overline{G}}(A) = \overline{C} = \overline{G\Phi(G)},$$

where the first equality holds since A acts trivially on \overline{G} . It follows that $G = G\Phi(G)$, and thus $G = C$ by the usual argument. (If $C < G$, then C is contained in some maximal subgroup of G , which necessarily contains $\Phi(G)$ too, and this is a contradiction.) ■

3.30. Corollary. *Let A act via automorphisms on G , where A and G are finite groups, and assume that $(|A|, |G|) = 1$ and that the action of A on G is faithful. Then the induced action of A on $G/\Phi(G)$ is faithful.*

Proof. Let $B = \mathbf{C}_A(G/\Phi(G))$ and apply the previous corollary to the action of B on G to deduce that $B = 1$. ■

Given an arbitrary group action on a finite set, there is an associated set of positive integers: the orbit sizes. Although there is very little that can be said about the sets of integers that arise in this way in general, the situation is quite different for actions via automorphisms on groups, where there is considerably more structure. (See, for example, Corollary 8.44.) For coprime actions, we can say even more. In that case, it is true that if m and n are coprime orbit sizes, then mn must also be an orbit size. To prove this, we use a remarkable observation of B. Hartley and A. Turull, which allows us to replace the group being acted on by an abelian group. The key step is the next theorem, which follows fairly easily from results about coprime actions that we have already established.

3.31. Theorem (Hartley-Turull). *Let A act via automorphisms on G , where A and G are finite groups, and suppose that $(|A|, |G|) = 1$. Assume also that*

at least one of A or G is solvable. Then A acts via automorphisms on some abelian group H in such a way that every subgroup $B \subseteq A$ has equal numbers of fixed points on G and on H . Also, there is a size-preserving bijection from the set of A -orbits on G to the set of A -orbits on H .

We extract part of the proof as a separate lemma, which has other applications.

3.32. Lemma. *Let A act via automorphisms on G , where A and G are finite groups, and suppose that $(|A|, |G|) = 1$. Assume also that at least one of A or G is solvable. Let $C = \mathbf{C}_G(A)$, and suppose that $P \in \text{Syl}_p(G)$ is A -invariant. Then $P \cap C \in \text{Syl}_p(C)$.*

Proof. Let $S \in \text{Syl}_p(C)$, and note that S is A -invariant. By Corollary 3.25, some A -invariant Sylow p -subgroup Q of G contains S . By Theorem 3.23(b), we have $Q^c = P$ for some element $c \in C$, and thus

$$P \cap C = Q^c \cap C = (Q \cap C)^c \supseteq S^c.$$

The result now follows because $P \cap C$ is a p -subgroup of C that contains the Sylow p -subgroup S^c . ■

The following is a very general result about groups acting on finite sets.

3.33. Lemma. *Let A be a group that acts on finite sets Ω and Λ , and assume that each subgroup $B \subseteq A$ has equal numbers of fixed points in Ω and in Λ . Then there is a bijection $f : \Omega \rightarrow \Lambda$ such that $f(\alpha \cdot a) = f(\alpha) \cdot a$ for all $\alpha \in \Omega$ and $a \in A$. In particular, f maps A -orbits on Ω to A -orbits on Λ , and so the sets of orbit sizes in the two actions are identical.*

Proof. We prove the existence of f by induction on $|\Omega|$; the assertions about orbits are then immediate. Let $\mu \in \mathcal{U}$, where \mathcal{U} is an A -orbit of smallest possible size in Ω . Then $|A : A_\mu| = |\mathcal{U}|$, and by the minimality of $|\mathcal{U}|$, no subgroup properly containing A_μ can fix a point in Ω . By hypothesis, therefore, no such subgroup can fix a point in Λ . Also by hypothesis, A_μ fixes some point $\nu \in \Lambda$, and it follows that A_μ is the full stabilizer of ν in A , and we have $A_\mu = A_\nu$.

We now define f on \mathcal{U} by setting $f(\mu \cdot x) = \nu \cdot x$ for $x \in A$. This is well defined since if $\mu \cdot x = \mu \cdot y$, then $xy^{-1} \in A_\mu = A_\nu$, and thus $\nu \cdot x = \nu \cdot y$. Also, f is injective on \mathcal{U} since if $\nu \cdot x = \nu \cdot y$, then $xy^{-1} \in A_\nu = A_\mu$, and thus $\mu \cdot x = \mu \cdot y$. Furthermore, if $\alpha \in \mathcal{U}$, we can write $\alpha = \mu \cdot x$ for some element $x \in A$, and hence if $a \in A$, we have

$$f(\alpha \cdot a) = f(\mu \cdot (xa)) = \nu \cdot (xa) = (\nu \cdot x) \cdot a = f(\alpha) \cdot a.$$

Now let $\mathcal{V} = f(\mathcal{U})$, so that \mathcal{V} is the orbit of ν and $|\mathcal{V}| = |\mathcal{U}|$. By taking $B = 1$, we see that $|\Omega| = |\Lambda|$, and thus if $\mathcal{U} = \Omega$, we have $\mathcal{V} = \Lambda$ and there is

nothing further to prove. We can assume, therefore, that $\mathcal{U} < \Omega$ and $\mathcal{V} < \Lambda$, and we observe that A acts on $\Omega - \mathcal{U}$ and on $\Lambda - \mathcal{V}$.

We will argue that the hypotheses of the lemma are satisfied for the actions of A on $\Omega - \mathcal{U}$ and $\Lambda - \mathcal{V}$. Once this is established, the inductive hypothesis will guarantee the existence of an appropriate bijection from $\Omega - \mathcal{U}$ to $\Lambda - \mathcal{V}$, and this can be used to extend the definition of f to all of Ω .

If $B \subseteq A$, we wish to show that B has equal numbers of fixed points in $\Omega - \mathcal{U}$ and in $\Lambda - \mathcal{V}$, and for this purpose, it suffices to show that B has equal numbers of fixed points in \mathcal{U} and \mathcal{V} . This is clear, however, since for each element $a \in A$ and each point $\alpha \in \mathcal{U}$, we have $f(\alpha \cdot a) = f(\alpha) \cdot a$, and so a fixes α if and only if it fixes $f(\alpha)$. ■

Proof of Theorem 3.31. We proceed in two steps to prove the first part; the final assertion then follows by Lemma 3.33. First, we show that G can be replaced by a nilpotent group, and then we complete the proof by showing that if G is nilpotent, it can be replaced by an abelian group.

For each prime divisor p of $|G|$, choose an A -invariant Sylow p -subgroup of G , and let N be the nilpotent group constructed as the external direct product of the set \mathcal{P} of selected Sylow subgroups. Since A acts on P for each member $P \in \mathcal{P}$, there is a natural action of A on N , and we argue that $|\mathbf{C}_N(B)| = |\mathbf{C}_G(B)|$ for each subgroup $B \subseteq A$. Since an element of the direct product N is B -fixed if and only if each of its components is fixed, it is clear that

$$|\mathbf{C}_N(B)| = \prod_{P \in \mathcal{P}} |\mathbf{C}_P(B)|,$$

and thus for each prime p , the p -part of $|\mathbf{C}_N(B)|$ is equal to $|\mathbf{C}_P(B)| = |P \cap C|$, where $C = \mathbf{C}_G(B)$. But $P \cap C \in \text{Syl}_p(C)$ by Lemma 3.32, and thus $|P \cap C|$ is the p -part of $|C|$. This shows that $|\mathbf{C}_N(B)|$ and $|C|$ have equal p -parts for all primes p , and hence $|\mathbf{C}_N(B)| = |C|$, as wanted.

To complete the proof, we can now assume that G is nilpotent, and in particular it is solvable with some derived length d . We proceed by induction on d . If $d = 1$, then G is abelian, and there is nothing to prove. We can thus assume that $d > 1$, and we define the external direct product $K = G' \times G/G'$, which has derived length $d - 1$. Since G' is characteristic in G , it is A invariant, and thus A acts via automorphisms on G' and on G/G' , and this induces an action via automorphisms of A on K . Since $|K| = |G'| |G/G'| = |G|$ is coprime to A , the inductive hypothesis applies, and thus there exists an abelian group H , acted on by A , and such that $|\mathbf{C}_H(B)| = |\mathbf{C}_K(B)|$ for every subgroup $B \subseteq A$.

It suffices now to show that $|C| = |\mathbf{C}_K(B)|$, where as before, $C = \mathbf{C}_G(B)$. Using Corollary 3.28 to obtain the second equality below, we obtain

$$\begin{aligned} |\mathbf{C}_K(B)| &= |\mathbf{C}_{G/G'}(B)| |\mathbf{C}_{G'}(B)| = |CG'/G'| |C \cap G'| \\ &= |C : C \cap G'| |C \cap G'| \\ &= |C|, \end{aligned}$$

and the proof is complete. ■

We can now prove the result about coprime orbit sizes that we mentioned earlier.

3.34. Theorem. *Let A act via automorphisms on G , where A and G are finite groups, and suppose that $(|A|, |G|) = 1$. Assume also that at least one of A or G is solvable. Suppose that there exist A -orbits of size m and n in G , where m and n are coprime. Then there is also an orbit of size mn .*

Proof. By Theorem 3.31, we can replace G by an abelian group of the same order without affecting orbit sizes, and thus we can assume that G is abelian. Now let \mathcal{X} and \mathcal{Y} be A -orbits in G of sizes m and n , respectively, and let $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. Then $|A : A_x| = |\mathcal{X}| = m$ and $|A : A_y| = |\mathcal{Y}| = n$, and since m and n are coprime, it follows by Lemma 3.16 that $A = A_x A_y$ and that $|A : A_x \cap A_y| = mn$. Now write $z = xy$, and observe that $A_x \cap A_y \subseteq A_z$. We will show that $A_x \cap A_y = A_z$, and consequently, the size of the A -orbit of z is $|A : A_x \cap A_y| = mn$. We work in the next few paragraphs to prove that $A_z \subseteq A_y$. Similar reasoning then shows that $A_z \subseteq A_x$, and this will complete the proof.

Define the map $\tau : G \rightarrow G$ by setting

$$\tau(g) = \prod_{a \in A_y} g^a.$$

Because G is abelian, the order of the factors in the product is irrelevant, and thus τ is well defined. Furthermore, and also because G is abelian, τ is a group homomorphism. We argue that τ maps each element of the orbit \mathcal{X} into $\mathbf{C}_G(A)$. To see this, recall that $A = A_x A_y$, and so A_y acts transitively on the set \mathcal{X} . If $u \in \mathcal{X}$, therefore, then as a runs over the elements of A_y , each element of \mathcal{X} occurs equally often in the form u^a . We conclude that $\tau(u)$ is a power of the product of the elements of the orbit \mathcal{X} , and thus $\tau(u)$ is A -invariant, as claimed.

Let $X = \langle \mathcal{X} \rangle$ and $Y = \langle \mathcal{Y} \rangle$, so that X and Y are A -invariant subgroups of G . Also, since τ is a homomorphism that maps every element of \mathcal{X} into $\mathbf{C}_G(A)$, it follows that $\tau(X)$ consists of A -fixed elements. Let $Z = X \cap Y$, and note that Z is also an A -invariant subgroup of G . Let $B \subseteq A$ be the (setwise) stabilizer of the coset Zy , and observe that $A_y \subseteq B$ since

A_y stabilizes both Z and y . Since B stabilizes the coset Zy , it follows by Theorem 3.27 that Zy contains a B -invariant element c , and thus $y \in Zc$ and we can write $y = tc$ for some element $t \in Z$.

Since c is B -invariant and $A_y \subseteq B$, we see that $\tau(c) = c^{|A_y|}$, and so $\tau(c)$ is B -invariant. Also, since $t \in Z \subseteq X$, we know that $\tau(t)$ is A -invariant, and in particular, it is B -invariant. We conclude that $y^{|A_y|} = \tau(y) = \tau(t)\tau(c)$ is B -invariant. Since $|A_y|$ is coprime to $|G|$, however, it follows that y is a power of $y^{|A_y|}$, and hence y is B -invariant and $B \subseteq A_y$.

We argue next that $A_z \subseteq B$, and thus $A_z \subseteq A_y$. To see this, note that $z = xy \in Xy$, and thus $Xy = Xz$, and this coset is stabilized by A_z . Since $y \in Y$, it is easy to check that $Xy \cap Y = (X \cap Y)y = Zy$, and since A_z stabilizes both Xy and Y , we conclude that A_z stabilizes Zy , and so $A_z \subseteq B$, as claimed. We have now shown that $A_z \subseteq A_y$, and as we remarked earlier, similar reasoning yields $A_z \subseteq A_x$. This completes the proof. ■

We mention that in the proof of Theorem 3.34, the orbit of $z = xy$ is exactly the set \mathcal{XY} . This is easy to see, but this observation does not yield a trivial proof of the theorem because it is not obvious that $|\mathcal{XY}| = |\mathcal{X}||\mathcal{Y}|$.

We close this section with one additional remark. Given an arbitrary set \mathcal{N} of integers exceeding 1, one can construct a graph with vertex set \mathcal{N} by creating an edge joining m and n in \mathcal{N} whenever m and n have a common prime divisor. An immediate consequence of Theorem 3.34 is that if \mathcal{N} is the set of nontrivial orbit sizes of a coprime finite group action, then the maximum distance between any two points in this graph is 2. For a not-necessarily coprime group action, it is still possible to say something about the corresponding graph: it has at most two connected components. (This theorem of the author and C. Praeger is presented in Chapter 8.)

Problems 3E

3E.1. Let A act on G via automorphisms, and assume that at least one of A or G is solvable, but do not assume that A and G have coprime orders. If G is nontrivial, prove that G contains a nontrivial A -invariant p -subgroup for some prime p .

Hint. If $P \triangleleft A$ is a p -subgroup and $C_G(P) = 1$, show that p does not divide $|G|$. Show in this situation that for each prime q , there is an A -invariant Sylow q -subgroup in G .

3E.2. Let A act via automorphisms on G , and assume that $(|A|, |G|) = 1$ and that at least one of A or G is solvable. Suppose that $G = HK$, where

H and K are A -invariant subgroups. Show that $C = (C \cap H)(C \cap K)$, where $C = \mathbf{C}_G(A)$.

Note. Wearing magic glasses, H and K are visible. The fact that $G = HK$ means that every element of G is the product of an element of H with an element of K . This problem asserts that this is visible through A -glasses. Every element of G that we can see is the product of a visible element of H with a visible element of K .

3E.3. Let A act on G via automorphisms, and let $N \triangleleft G$ be A -invariant. Assume that $(|A|, |N|) = 1$ and that A acts trivially on both N and G/N . Show that A acts trivially on G .

Hint. No solvability assumption is needed here because it is no loss to assume that A is cyclic.

3E.4. In the usual coprime action situation with A acting on G , let $C = \mathbf{C}_G(A)$. If $H \subseteq G$ is A -invariant, show that $|H : H \cap G|$ divides $|G : C|$ and that $|G : C \cap H|$ divides $|G : H|$.

Hint. Use Lemma 3.32.

3E.5. Let G be p -solvable, and assume that $\mathbf{O}_{p'}(G) = 1$. Let $P = \mathbf{O}_p(G)$ and write $F = \Phi(P)$, so that $F \triangleleft G$. Note that there is a natural action of G on P/F , and observe that P is contained in the kernel of this action since P/F is abelian. Show that P is the full kernel of this action.

Note. In other words, G/P acts faithfully on P/F , and so G/P is isomorphic to a subgroup of $\text{Aut}(P/F)$. Also, P/F is an elementary abelian p -group, of order p^n , say, and so it is isomorphic to the additive group of an n -dimensional vector space over a field of order p . It follows that G/P is isomorphic to a group of invertible $n \times n$ matrices over this field.

3F

We close this already long chapter on split extensions with a discussion of certain extensions that are not generally split. Given a group N and a positive integer m , we wish to construct all (up to isomorphism) groups G , where G has a normal subgroup $N_0 \cong N$ such that G/N_0 is cyclic of order m . As was the case when we discussed semidirect products earlier in this chapter, our “synthesis” will be preceded by some “analysis” that will enable us to understand groups of the type we wish to construct.

Suppose $N \triangleleft G$ and that G/N is cyclic of order m . Let gN be a coset that generates the cyclic group G/N , and observe that $g^m \in N$. It should be clear that the element g^m of N and the automorphism of N induced by g

are relevant to this situation, and in fact, these two objects, along with the group N and the integer m uniquely determine G up to isomorphism. In the following, we will again use the convention that if $N \cong N_0$, then $x \in N$ and $x_0 \in N_0$ are corresponding elements under the given isomorphism.

3.35. Theorem. *Let G and G_0 be groups, and let $N \triangleleft G$ and $N_0 \triangleleft G_0$, where G/N and G_0/N_0 are cyclic of finite order m . Suppose that $n \mapsto n_0$ is an isomorphism from N to N_0 , and let gN and g_0N_0 be generating cosets of G/N and G_0/N_0 respectively. Assume that*

$$(g^m)_0 = (g_0)^m \quad \text{and} \quad (x^g)_0 = (x_0)^{g_0}$$

for all elements $x \in N$. Then there is a unique isomorphism $\theta : G \rightarrow G_0$ that extends the given isomorphism $N \rightarrow N_0$ and that carries g to g_0 .

Proof. The distinct cosets of N in G are g^iN with $0 \leq i < m$, and so each element $u \in G$ is uniquely of the form $u = g^i x$ for some element $x \in N$ and some integer i in this range. We are therefore forced to define θ by setting $\theta(u) = \theta(g^i x) = (g_0)^i x_0$, and we must show that θ is indeed an isomorphism from G onto G_0 . The elements of G_0 are uniquely of the form $(g_0)^i x_0$ for $0 \leq i < m$, and it follows easily that θ is both injective and surjective.

It remains to prove that θ is a homomorphism. We show first that $\theta(g^i x) = (g_0)^i x_0$ for $x \in N$, and without restriction on the integer i . Write $i = qm + r$, where $0 \leq r < m$. By hypothesis, $g^m \in N$ and $(g^m)_0 = (g_0)^m$, and thus $((g^m)^q x)_0 = (g_0)^{mq} x_0$. We have

$$\theta(g^i x) = \theta(g^r (g^m)^q x) = (g_0)^r ((g^m)^q x)_0 = (g_0)^{mq+r} x_0 = (g_0)^i x_0,$$

as wanted. Now $g^i x g^j y = g^{i+j} x^{g^j} y$ for integers i and j and elements $x, y \in N$. Since $(x^{g^j})_0 = (x_0)^{(g_0)^j}$, it is easy to compute that $\theta((g^i x)(g^j y)) = \theta(g^i x)\theta(g^j y)$. This completes the proof. ■

Now suppose that we are given four ingredients: a group N , a positive integer m , an element $a \in N$ and an automorphism σ of N . The previous theorem guarantees that up to isomorphism, there is at most one group G having N as a normal subgroup with cyclic factor group G/N of order m , and having generating coset gN , where $g^m = a$ and $x^g = x^\sigma$ for all $x \in N$.

But given N and m , not every choice of $a \in N$ and $\sigma \in \text{Aut}(N)$ correspond to an actual group. If the group G exists, then since conjugation by g effects the automorphism σ on N , and $a = g^m$ is fixed by g , we must have $a^\sigma = a$. Another condition that clearly must be satisfied is that the m th power of the automorphism σ must be the inner automorphism induced by a . As the following cyclic extension theorem shows, there are no further requirements.

3.36. Theorem. *Let N be a group and m a positive integer, and let $a \in N$ and $\sigma \in \text{Aut}(N)$. Assume that*

$$a^\sigma = a \quad \text{and} \quad x^{\sigma^m} = x^a$$

for all $x \in N$. Then there exists a group G , unique up to isomorphism, and having N as a normal subgroup with the following properties.

- (a) $G/N = \langle gN \rangle$ is cyclic of order m .
- (b) $g^m = a$.
- (c) $x^\sigma = x^g$.

Proof. The uniqueness follows by Theorem 3.35, and so it suffices to construct G , which we do by realizing it within the symmetric group on the set Ω of ordered pairs (i, y) , where $0 \leq i < m$ and $y \in M$. First, we define an action of N on Ω by setting $(i, y) \cdot x = (i, yx)$, where $0 \leq i < m$ and $x, y \in N$. It is trivial to check that this defines a faithful action, and so we get a corresponding isomorphism $N \rightarrow N_0 \subseteq \text{Sym}(\Omega)$, where x_0 is the permutation effected by x for $x \in N$. For convenience, we identify N with N_0 via this isomorphism, so that $N \subseteq \text{Sym}(\Omega)$.

Next, we define a function $g : \Omega \rightarrow \Omega$ by setting $(i, y)g = (i + 1, y^\sigma)$ for $0 \leq i < m - 1$ and $y \in N$, and $(m - 1, y)g = (0, ay^\sigma)$. Since $a^\sigma = a$ and σ is an automorphism, we see that $(i, ay)g = (i + 1, ay^\sigma)$ for $0 \leq i < m - 1$, and it follows easily that

$$(i, y)g^m = (i, ay^{\sigma^m}) = (i, ay^a) = (i, ya) = (i, y)a$$

for all $(i, y) \in \Omega$. (To check the first equality, observe that each application of g increases the first component by 1 modulo m . We pick up one extra factor of a when the first component changes from $m - 1$ to 0, and that factor is unaffected by additional applications of the function g .) Thus $g^m = a$, and in particular, g is a permutation of Ω .

We show next that $xg = gx^\sigma$ for all $x \in N$. To verify this, it suffices to check that these functions have the same effect on each element (i, y) of Ω , and so we want $((i, y)x)g = ((i, y)g)x^\sigma$. If $0 \leq i < m - 1$, we have

$$((i, y)x)g = (i, yx)g = (i + 1, (yx)^\sigma) = (i + 1, y^\sigma x^\sigma) = ((i, y)g)x^\sigma,$$

and also

$$((m - 1, y)x)g = (m - 1, yx)g = (0, a(yx)^\sigma) = (0, ay^\sigma x^\sigma) = (m - 1, y)gx^\sigma,$$

as wanted. It follows that $x^g = x^\sigma$, and in particular, $N \triangleleft G$, where $G = \langle N, g \rangle$. Also, G/N is cyclic, with generating coset gN .

All that remains to check is that G/N has order m . Since $g^m = a \in N$, it suffices to show that $g^j \notin N$ for $0 < j < m$. But $(0, 1)g^j = (j, 1)$ and

$(0, 1)x = (0, x)$ for $x \in N$, and thus g^j cannot be an element $x \in N$ when $0 < j < m$. This completes the proof. ■

As an example of the use of the cyclic extension theorem, we give another construction of the generalized quaternion groups. We saw these previously, in Problem 3A.2, where they were constructed as index-2 subgroups of semidihedral groups.

Given a positive integer n , divisible by 8, we start with a cyclic group N of order $n/2$. Let a be the unique element of N of order 2 and let $\sigma \in \text{Aut}(N)$ be the map $x \mapsto x^{-1}$, so that σ fixes a . Taking $m = 2$, we see that σ^m is the trivial automorphism of N , and so it is equal to the inner automorphism induced by a . By the cyclic extension theorem, therefore, the cyclic group N can be embedded as a normal subgroup with index $m = 2$ in a group Q , and there exists an element $g \in Q - N$ such that $g^2 = a$ and $x^g = x^{-1}$ for all $x \in N$. We argue that every element of $Q - N$ has order 4, and thus a is the only element of order 2 in Q . To see this, observe that all elements of $Q - N$ have the form gx with $x \in N$, and we have $(gx)^2 = gxgx = g^2x^gx = ax^{-1}x = a$, which has order 2. Thus gx has order 4, as claimed. The unique group constructed here is denoted Q_n ; it is the **generalized quaternion** group of order n . (See the remark concerning nomenclature following Problem 3A.2.)

Problems 3F

3F.1. Let G be a group of order n divisible by 8, and suppose that N has a cyclic subgroup C of index 2 such that every element of $G - C$ has order 4. Show that $G \cong Q_n$, the generalized quaternion group.

3F.2. Show that in principle, we can construct every solvable group by starting with the trivial group and repeatedly applying Theorem 3.36.

3F.3. Let $Q = Q_8$. Show that Q has exactly three cyclic subgroups of order 4, and that these are transitively permuted by $\text{Aut}(Q)$.

Hint. If A and B are cyclic subgroups of Q of order 4, use Theorem 3.35 to construct an isomorphism from Q to Q that carries A to B .

3F.4. Let $S = SL(2, 3)$, which is the group of 2×2 matrices of determinant 1 over the integers modulo 3. Show that $|S| = 24$ and that it has a normal Sylow 2-subgroup isomorphic to Q_8 .

3F.5. Let $S = SL(2, 3)$ as in the previous problem, and note that S has index 2 in $G = GL(2, 3)$, the full group of invertible 2×2 matrices over the integers modulo 3. Show that $G - S$ contains an element g of order 2, but

that it contains no element of order 4. Prove that there exists a group H containing S as a subgroup of index 2, where $H - S$ contains an element h of order 4 such that the automorphisms of S induced by g in G and by h in H are identical. Show that $H - S$ contains no element of order 2 and finally, show that both $G - S$ and $H - S$ contain elements of order 8.

Commutators

4A

We begin with a bit of review. The commutator of two elements x and y in a group G is the element $x^{-1}y^{-1}xy$, which is denoted $[x, y]$. Since $[x, y] = (yx)^{-1}xy$, we can think of the commutator of x and y as the “difference” between yx and xy , and in particular, $[x, y] = 1$ if and only if x and y commute. Alternatively, we can write $[x, y] = x^{-1}x^y$, so $[x, y]$ can also be viewed as the “difference” between x and its conjugate x^y .

If $H \subseteq G$ and $K \subseteq G$ are subgroups, we write $[H, K]$ to denote the subgroup generated by the set $\{[h, k] \mid h \in H, k \in K\}$ of all commutators of elements of H with elements of K . This subgroup is the **commutator** of H and K , and it is trivial if and only if H and K centralize each other. We stress that, in general, $[H, K]$ is not *equal* to the set of commutators of elements of H with elements of K ; it is the group *generated* by them, or equivalently, it is the unique smallest subgroup of G that contains all of these commutators. In particular, the subgroup $[G, G]$, which is generated by all commutators in G , need not consist entirely of commutators. Recall that this subgroup is usually denoted G' ; it is the derived subgroup (or commutator subgroup) of G . The derived subgroup G' of G is trivial if and only if G is abelian, and as we know, it is the unique normal subgroup of G minimal with the property that the corresponding factor group is abelian.

There are a number of useful identities satisfied by commutators. It is trivial to check, for example, that $[x, y][y, x] = 1$ for all $x, y \in G$. In other words, $[y, x] = [x, y]^{-1}$, and so if $H, K \subseteq G$, then the generating commutators of $[K, H]$ are exactly the inverses of the generating commutators of $[H, K]$, and it follows that $[K, H] = [H, K]$. Another often-used identity,

which the reader should check, is that $[xy, z] = [x, z]^y[y, z]$ for all $x, y, z \in G$. (In the language of Section 3B, this says that for each element $z \in G$, the map $[\cdot, z]$ from G to G is a crossed homomorphism with respect to the conjugation action of G on itself.) This identity is the key, for example, to proving the following fact.

4.1. Lemma. *Let H and K be subgroups of a group G . Then H and K normalize $[H, K]$, or equivalently, $[H, K] \triangleleft \langle H, K \rangle$, the subgroup generated by H and K .*

Proof. Since $[H, K] = [K, H]$, it suffices by symmetry to prove that $H \subseteq \mathbf{N}_G([H, K])$. Let $h, x \in H$ and $k \in K$. Then $[hx, k] = [h, k]^x[x, k]$, and so $[h, k]^x = [hx, k][x, k]^{-1} \in [H, K]$. In other words, conjugation by $x \in H$ maps each of the generators $[h, k]$ of $[H, K]$ back into $[H, K]$, and thus $[H, K]^x \subseteq [H, K]$. It follows that $[H, K]^x = [H, K]$, as wanted. (As usual, we substitute x^{-1} for x to deduce the reverse containment.) ■

Not surprisingly, there is a formula for $[z, xy]$ analogous to the identity $[xy, z] = [x, z]^y[y, z]$, but it seems pointless to memorize it since it can easily be derived using the formula for $[xy, z]$. To be specific, we have the following:

$$[z, xy] = [xy, z]^{-1} = ([x, z]^y[y, z])^{-1} = [y, z]^{-1}([x, z]^y)^{-1} = [z, y][z, x]^y.$$

We have already said that K centralizes H if and only if $[H, K] = 1$. This can be generalized slightly, as follows.

4.2. Lemma. *Let N be a normal subgroup of a group G , and suppose that $H, K \subseteq G$ are arbitrary subgroups. Write $\overline{G} = G/N$ and follow the standard “bar convention”, so that \overline{H} and \overline{K} are the images of H and K in \overline{G} under the canonical homomorphism $G \rightarrow \overline{G}$. Then $[\overline{H}, \overline{K}] = [\overline{H}, \overline{K}]$, and in particular, \overline{H} and \overline{K} centralize each other in \overline{G} if and only if $[H, K] \subseteq N$.*

Proof. Since overbar is a homomorphism, we have $[\overline{u}, \overline{v}] = \overline{[u, v]}$ for arbitrary elements $u, v \in G$, and it follows that $[\overline{H}, \overline{K}] = \overline{[H, K]}$. This subgroup is trivial precisely when $[H, K] \subseteq N$. ■

We can also express the relation “ K normalizes H ” in the language of commutators.

4.3. Lemma. *Let H and K be subgroups of a group G . Then $K \subseteq \mathbf{N}_G(H)$ if and only if $[H, K] \subseteq H$. In particular, $H \triangleleft G$ if and only if $[H, G] \subseteq H$.*

Proof. Let $h \in H$ and $k \in K$. Since $[h, k] = h^{-1}h^k$, we have $h^k = h[h, k]$, and thus $h^k \in H$ if and only if $[h, k] \in H$. The result is now immediate. ■

If H and K normalize each other, therefore, then $[H, K] \subseteq H \cap K$. If also $H \cap K = 1$, then $[H, K] = 1$, and so H and K centralize each other. (We have seen and used this fact previously.)

We can use Lemmas 4.2 and 4.3 to reexamine the notion of a central series in a group. Recall that a series of subgroups

$$1 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_r = G$$

is a central series in G if all H_i are normal in G , and also $H_i/H_{i-1} \subseteq \mathbf{Z}(G/H_{i-1})$ for $0 < i \leq r$. By Lemma 4.2, the latter condition can be restated as $[H_i, G] \subseteq H_{i-1}$ for $0 < i \leq r$. Conversely, suppose we have a series of subgroups H_i , as above, and assume that $[H_i, G] \subseteq H_{i-1}$ for $0 < i \leq r$. First, observe that since $H_{i-1} \subseteq H_i$, we have $[H_i, G] \subseteq H_i$, and thus Lemma 4.3 yields $H_i \triangleleft G$ for all i . The subgroups H_i thus form a normal series, and indeed they form a central series by Lemma 4.2.

To continue this discussion of central series, it is convenient to define commutators of three or more elements or of three or more subgroups. The standard notational convention is to use “left association”. For three elements, for example, the triple commutator is defined by $[x, y, z] = [[x, y], z]$, and for three subgroups, the definition is $[X, Y, Z] = [[X, Y], Z]$. (Caution: in general it is not true that $[X, Y, Z]$ is generated by the elements of the form $[x, y, z]$ with $x \in X$, $y \in Y$ and $z \in Z$.) More generally, for $n > 2$, we define

$$[x_1, x_2, \dots, x_n] = [[x_1, x_2, \dots, x_{n-1}], x_n].$$

and similarly for subgroups.

Now suppose that $\{H_i \mid 0 \leq i \leq r\}$ is a central series for G , as before. Then

$$[G, G] = [H_r, G] \subseteq H_{r-1},$$

and thus if $r \geq 2$, we have

$$[G, G, G] = [[G, G], G] \subseteq [H_{r-1}, G] \subseteq H_{r-2},$$

and if $r \geq 3$,

$$[G, G, G, G] = [[G, G, G], G] \subseteq [H_{r-2}, G] \subseteq H_{r-3}.$$

Continuing like this, we see that if $k \leq r + 1$, then $[G, G, \dots, G] \subseteq H_{r-k+1}$, where there are k copies of G in the commutator on the left.

Clearly, we need some better notation here, and so we write $G^1 = G$, $G^2 = [G, G]$, $G^3 = [G, G, G]$ and in general, $G^k = [G^{k-1}, G]$ for $k > 1$. (This notation is not completely standard; some authors write $\gamma^k(G)$ to denote our subgroup G^k , and one can find other notations in the literature too.) Note that $G^2 = [G, G] = G'$, the derived subgroup, but in general, G^k with $k > 2$ is not one of the groups $G^{(m)}$ of the derived series, and in particular,

$G^{(2)} = G'' = [[G, G], [G, G]]$ is not usually one of our subgroups G^k . (We shall see, however, that $G'' \subseteq G^4$, and in general, $G^{(k)} \subseteq G^{2^k}$.)

Note that the subgroups G^k are characteristic in G . In particular, $G^k \triangleleft G$, and so by Lemma 4.3, we have $G^{k+1} = [G^k, G] \subseteq G^k$. The subgroups G^k , therefore, form a descending series. (Another way to see this is by induction on k . Assuming that $G^k \subseteq G^{k-1}$, we get $G^{k+1} = [G^k, G] \subseteq [G^{k-1}, G] = G^k$.)

Returning now to the subgroups H_i of our central series for G , we have $G^k \subseteq H_{r-k+1}$ for $1 \leq k \leq r+1$, and in particular, $G^{r+1} \subseteq H_0 = 1$. Now consider an arbitrary nilpotent group, which, we recall, simply means that G has a central series. It follows that $G^m = 1$ for some positive integer m . More precisely, if G is nilpotent and has a central series of length r , then $G^{r+1} = 1$. (The length of a series is the number of containments.)

Conversely, suppose that $G^m = 1$ for some positive integer m . Consider the series

$$1 = G^m \subseteq G^{m-1} \subseteq \dots \subseteq G^1 = G.$$

(Note that the numbering of these subgroups is “backwards”, running from high to low.) Since $[G^k, G] = G^{k+1}$, it follows that this is a central series, and thus G is nilpotent. Furthermore, we have seen that $G^k \subseteq H_{r-k+1}$, where the H_i form an arbitrary central series in G . Since the G^k are contained term-by-term in the subgroups of an arbitrary central series, the series of G^k is called the **lower central series** of G . The length of this series is, of course $m-1$, where m is the smallest positive integer such that $G^m = 1$.

Recall from Chapter 1 that the nilpotence class of a nilpotent group G is the smallest integer r such that G is equal to the term Z_r of the upper central series of G . We saw that it is also the smallest integer r such that G has a central series $\{H_i \mid 0 \leq i \leq r\}$, with $H_0 = 1$ and $H_r = G$. (In other words, the nilpotence class is the length of the shortest possible central series.) We now know that if G is nilpotent of class r then $G^{r+1} = 1$. Also, it is not possible that $G^m = 1$ with $m < r+1$ because otherwise, the lower central series of G would be a central series of length $m-1 < r$. This shows that if G is nilpotent of class r , then $m = r+1$ is the smallest integer such that $G^m = 1$.

Of course, if G is an arbitrary (and not necessarily nilpotent) group, one can still consider subgroups of the form $G^m = [G, G, \dots, G]$, where G occurs m times. By abuse of notation, the series $\{G^i \mid i \geq 1\}$ is often called the “lower central series” of G , even though in the nonnilpotent case, it is not a true central series because the identity is not one of its terms. If G is finite, then since its lower central series cannot involve infinitely many strict containments, there must be some superscript m such that $G^m = G^{m+1}$. It is then immediate that $G^m = G^n$ for all integers $n \geq m$, and this final term of the lower central series of G is denoted G^∞ . It is not hard to see

that if $N \triangleleft G$, then G/N is nilpotent if and only if $G^\infty \subseteq N$. (To see this, write $\overline{G} = G/N$, and observe that $\overline{G^m} = \overline{G}^m$ by repeated application of Lemma 4.2.) It follows that if G is finite, then G^∞ is the unique normal subgroup of G minimal with the property that the corresponding factor group is nilpotent.

As we mentioned in Chapter 1, the groups of nilpotence class 1 are exactly the nontrivial abelian groups. Somewhat more interesting are groups of nilpotence class 2. For these nonabelian groups, we have $1 = G^3 = [G, G, G] = [G', G]$, so that the derived subgroup $G' \subseteq \mathbf{Z}(G)$, or equivalently $G/\mathbf{Z}(G)$, is abelian. In this case, all commutators are central, and hence $[xy, z] = [x, z]^y[y, z] = [x, z][y, z]$, and so the map $[\cdot, z]$ defines a homomorphism from G into G' . The following easy consequence of this is sometimes useful. (Before we state our result, we recall that the **exponent** of a group G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$. In other words, the exponent of a group is the least common multiple of the orders of its elements.)

4.4. Lemma. *Let P be a p -group of nilpotence class 2, and assume that P' has exponent p^e . Then the exponent of $P/\mathbf{Z}(P)$ divides p^e . In particular, if P' is elementary abelian, then $P/\mathbf{Z}(P)$ is elementary abelian, and thus $\Phi(P) \subseteq \mathbf{Z}(P)$.*

Note that if P has class 2, then $P' \subseteq \mathbf{Z}(P)$, and so both P' and $P/\mathbf{Z}(P)$ are abelian. Thus P' is elementary abelian if and only if $e = 1$, and to prove that $P/\mathbf{Z}(P)$ is elementary abelian, it suffices to show that its exponent divides p , and this is the assertion of the lemma when $e = 1$. The last conclusion of the lemma, therefore, is an immediate consequence of the characterization of the Frattini subgroup of a p -group as the unique smallest normal subgroup having an elementary abelian factor group. This fact was mentioned previously, but we never gave a formal proof, and so we digress to do so now.

4.5. Lemma. *Let $N \triangleleft P$, where P is a p -group. Then P/N is elementary abelian if and only if $\Phi(P) \subseteq N$.*

Proof. Let $M < P$ be a maximal subgroup. Since P is nilpotent, $M \triangleleft P$, and we see that P/M has no subgroups other than itself and the identity. Thus P/M has prime order, which must be p . Now P/M is abelian, and so $P' \subseteq M$, and also, given $x \in P$, we have $x^p \in M$. Thus P' and x^p lie in the intersection of all maximal subgroups of G , or in other words, they lie in $\Phi(P)$. We conclude that $P/\Phi(P)$ is elementary abelian, and thus also P/N is elementary abelian if $\Phi(P) \subseteq N \subseteq P$.

Conversely, suppose P/N is elementary abelian, and assume that $N < P$. By the fundamental theorem of abelian groups, P/N is a direct product of

nontrivial cyclic subgroups, each of which must have order p . The product of all but one of these factors has index p , and so is maximal in P/N . The intersection of those maximal subgroups of P/N obtained by deleting one of its direct factors of order p is trivial, and thus N is the intersection of some collection of maximal subgroups of P . We conclude that $\Phi(P) \subseteq N$, as wanted. ■

Proof of Lemma 4.4. To prove that $P/\mathbf{Z}(P)$ has exponent dividing p^e , we must show that $x^{p^e} \in \mathbf{Z}(P)$ for all $x \in P$. We have $[x^{p^e}, y] = [x, y]^{p^e} = 1$, where the first equality holds since $[\cdot, y]$ is a homomorphism, and of course, the second equality holds because $[x, y] \in P'$, which has exponent p^e . This shows that x^{p^e} commutes with all elements $y \in P$, and so $x^{p^e} \in \mathbf{Z}(P)$, as required. By Lemma 4.5, the proof is now complete. ■

Next, we present a result relating centers and commutator subgroups. Its proof is based on an exception to the general principle that elements of the commutator subgroup need not be commutators.

4.6. Lemma. *Let A be an abelian normal subgroup of a group G , and suppose that G/A is cyclic. Then $G' = [A, G]$ and*

$$G' \cong A/(A \cap \mathbf{Z}(G)).$$

In particular, if A is finite, then $|A| = |G'| |A \cap \mathbf{Z}(G)|$.

Proof. Choose a generating coset Ag for G/A , and let $\theta : A \rightarrow A$ be the map defined by $\theta(a) = [a, g]$. (Note that $[a, g] \in A$ since $A \triangleleft G$.) If $a, b \in A$, then

$$\theta(ab) = [ab, g] = [a, g]^b [b, g] = [a, g][b, g] = \theta(a)\theta(b),$$

where the third equality holds since $[a, g]$ and b lie in the abelian group A . Thus θ is a homomorphism, and $\ker(\theta) = \mathbf{C}_A(g)$. Also, $\theta(A)$ is a subgroup, and $\theta(A) \subseteq [A, G] \subseteq G'$.

Since Ag is a generating coset for $\overline{G} = G/A$, we see that $\langle \overline{g} \rangle = \langle \overline{g} \rangle = \overline{G}$, and thus $G = A\langle g \rangle$, and it follows that $\mathbf{C}_A(g) \subseteq A \cap \mathbf{Z}(G)$. The reverse inequality is clear, and thus $\ker(\theta) = \mathbf{C}_A(g) = A \cap \mathbf{Z}(G)$. This yields $\theta(A) \cong A/(A \cap \mathbf{Z}(G))$, and so to complete the proof, it suffices to show that $\theta(A) = G'$.

We already know that $\theta(A)$ is a subgroup of G' , and so it suffices to show that $\theta(A) \triangleleft G$ and that $G/\theta(A)$ is abelian. First, since A is abelian and $\theta(A) \subseteq A$, it is clear that $A \subseteq \mathbf{N}_G(\theta(A))$. Also, $\theta(a)^g = [a, g]^g = [a^g, g] = \theta(a^g) \in \theta(A)$ for all $a \in A$, and thus $g \in \mathbf{N}_G(\theta(A))$. It follows that $G = A\langle g \rangle \subseteq \mathbf{N}_G(\theta(A))$, and so $\theta(A) \triangleleft G$, as required.

Now (redefining overbars) write $\overline{G} = G/\theta(A)$, so that $\overline{G} = \overline{A}\langle \overline{g} \rangle$. Since $[\overline{a}, \overline{g}] = [\overline{a}, \overline{g}] = \overline{\theta(a)}$ is trivial for all $a \in A$, it follows that the elements \overline{a} for

$a \in A$ together with \bar{g} form a pairwise commuting set of generators for \bar{G} , which is therefore abelian. This completes the proof. ■

As an example of how Lemma 4.6 can be used, we offer the following.

4.7. Theorem. *Let $A \triangleleft P$, where P is a p -group, and suppose that A is abelian and $|A| = p^m$. Assume that P/A is cyclic, and that $|A \cap \mathbf{Z}(P)| = p$. Then the nilpotence class of P is m .*

Proof. Let $Z = A \cap \mathbf{Z}(P)$, and note that $P' \subseteq A$ and $|A : P'| = |Z| = p$ by Lemma 4.6. If $m = 1$, then $A = Z$ is central in P , and since P/A is cyclic, it follows that P is abelian, and thus its nilpotence class is $1 = m$, as wanted. We can thus assume that $m > 1$, and we proceed by induction on m .

Since $|A : P'| = p$ and $|A| > p$, we have $P' > 1$, and thus P' meets $\mathbf{Z}(P)$ nontrivially by Theorem 1.19. Then $1 < P' \cap \mathbf{Z}(P) \subseteq A \cap \mathbf{Z}(P) = Z$, and since $|Z| = p$, we have $Z = P' \cap \mathbf{Z}(P)$, and in particular, $Z \subseteq P'$. Now write $\bar{P} = P/Z$, and observe that $(\bar{P})' = \bar{P}'$ has index p in the abelian normal subgroup \bar{A} of \bar{P} . Also, $\bar{P}/\bar{A} \cong P/A$ is cyclic, and hence by Lemma 4.6, we have $|\bar{A} \cap \mathbf{Z}(\bar{P})| = |\bar{A} : (\bar{P})'| = p$, and thus \bar{P} satisfies the hypotheses of the theorem.

Since $|\bar{A}| = p^{m-1}$, we conclude from the inductive hypothesis that \bar{P} has nilpotence class $m - 1$, and thus in the lower central series of \bar{P} , we have $(\bar{P})^m = 1$ and $(\bar{P})^{m-1} \neq 1$. Since $\bar{P}^m = (\bar{P})^m = 1$, we have $P^m \subseteq Z$, and thus $P^{m+1} = [P^m, P] \subseteq [Z, P] = 1$.

To complete the proof, we must show that $P^m \neq 1$. If $m = 2$, then $P^m = P' > 1$, and so we can suppose that $m > 2$, and hence $P^{m-1} \subseteq P^2 = P' \subseteq A$. We have $\bar{P}^{m-1} = (\bar{P})^{m-1} \neq 1$, and thus $P^{m-1} \not\subseteq Z = A \cap \mathbf{Z}(P)$. It follows that $P^{m-1} \not\subseteq \mathbf{Z}(P)$, and thus $P^m = [P^{m-1}, P] \neq 1$, as required. ■

Suppose now that P is a nonabelian p -group of order p^e . Assume that $|\mathbf{Z}(P)| = p$, and that P has an abelian subgroup A of index p (which, of course, is necessarily normal). Since P is nonabelian, A is nontrivial, and thus $A \cap \mathbf{Z}(P) > 1$, and hence $\mathbf{Z}(P) \subseteq A$. Also, P/A is cyclic, and it follows by Theorem 4.7 that the nilpotence class of P is $e - 1$.

To put this into context, let P be an arbitrary p -group of nilpotence class r , and order p^e , where $e \geq 2$. Since P has at least one normal subgroup of index p^2 and the corresponding factor group is abelian, it follows that $|P : P'| \geq p^2$. Now consider the lower central series

$$P = P^1 > P^2 > P^3 > \dots > P^{r+1} = 1,$$

and observe that $|P : P^2| = |P : P'| \geq p^2$, and of course, $|P^i : P^{i+1}| \geq p$ for $2 \leq i \leq r$. Then $p^e = |P : P^{r+1}|$ is the product of r integers, each of which is at least p , and one of which is at least p^2 . It follows that $e \geq r + 1$, and

thus the nilpotence class r of a p -group P of order p^e with $e \geq 2$ is at most $e - 1$. If it happens that $r = e - 1$, we say that P has **maximal class**.

If $|P| = p^e \geq p^2$ and $|\mathbf{Z}(P)| = p$ and P has an abelian subgroup of index p , we have seen that P has nilpotence class $e - 1$, and thus P has maximal class. In particular, it is easy to see that dihedral, generalized quaternion and semidihedral 2-groups satisfy these hypotheses, and so all of these groups have maximal class. In fact, these are the only maximal class 2-groups, but we will not prove that here. Also, we mention without proof that for $p > 2$, there exist maximal class p -groups that fail to have an abelian subgroup of index p .

We close this section with a discussion of the set of elements $x \in P$ such that $x^p = 1$, where P is a p -group. In general, these elements do not form a subgroup. (If $P = D_8$, for example, there are exactly six such elements including the identity, and of course a set of six elements in a group of order 8 cannot be a subgroup.) The group generated by all elements $x \in P$ such that $x^p = 1$ is denoted $\Omega_1(P)$, and more generally, for integers $r \geq 1$, one defines $\Omega_r(P) = \langle x \in P \mid x^{p^r} = 1 \rangle$. (There does not seem to be any standard name for this characteristic subgroup, which is usually just called “omega- r ” of P .)

If $p > 2$ and P is a p -group of class at most 2, then the elements $x \in P$ such that $x^p = 1$ actually do form a subgroup. (Equivalently, $\Omega_1(P)$ has exponent dividing p in this case.) As is shown by D_8 , which has class 2, the condition $p > 2$ is essential. But the assumption that the nilpotence class is at most 2 is unnecessarily strong; in fact, it suffices to assume that the nilpotence class is less than the prime p . The proof of this result of Philip Hall uses “commutator collection”, which is the basic idea that underlies our proof for class 2 groups. The proof of the full result is considerably more complicated, however, and we do not present it here.

Given $x, y \in P$ with $x^p = 1 = y^p$, we want to show that $(xy)^p = 1$, and so we investigate how to compute $(xy)^n$ for arbitrary elements $x, y \in P$ and positive integers n . The idea here is as follows. We have

$$(xy)^n = xyxyxy \cdots xy$$

where on the right, there are n copies of x alternating with n copies of y . If P is abelian, it is trivial to simplify this. We can move each copy of x as far as necessary to its left, freely passing through the intervening copies of y , thereby collecting the n copies of x at the left, and leaving n copies of y on the right. This, of course, yields the familiar formula $(xy)^n = x^n y^n$ for abelian groups.

What if P is not abelian? In general, in any group, if we have the string yx and we want to move the x to the left, across the y , we can use the

identity $yx = xy[y, x]$. In other words, we can still pass the x through the y , but to do so, we must pay a price. The penalty is that we must insert the commutator $[y, x]$ to the right of the y .

For simplicity, consider the case $n = 3$. Moving the second x left across the first y (and inserting $[y, x]$ as payment for the privilege of doing this) we have

$$(xy)^3 = xyxyxy = xxy[y, x]yxy.$$

Next, we want to move the third x leftward in order to join the first two, and we do this in three steps, first moving across y , then across $[y, x]$, and finally across another y . To pay for these transits, we must insert $[y, x]$, and then $[y, x, x]$, and then another $[y, x]$. We thus have

$$\begin{aligned} (xy)^3 &= xyxyxy = xxy[y, x]yxy \\ &= xxy[y, x]xy[y, x]y \\ &= xxyx[y, x][y, x, x]y[y, x]y \\ &= xxxy[y, x][y, x][y, x, x]y[y, x]y, \end{aligned}$$

and at this point, we have collected all three copies of x at the left, and these are followed by a mixture consisting of three copies of y , three copies of $[y, x]$, and one copy of $[y, x, x]$.

We can now continue to “simplify” this, by collecting the three copies of y toward the left, to a position just to the right of the three copies of x . In order to do this, we will need to move the second y across copies of $[y, x]$ and $[y, x, x]$, and so we must pay penalties of $[y, x, y]$ and $[y, x, x, y]$. To collect the third y , our penalties will be $[y, x, y]$, $[y, x, x, y]$, and also $[y, x, y, y]$ and $[y, x, x, y, y]$. When this process is finished, we will have $(xy)^3 = x^3y^3w$, where w is some complicated product of one or more copies of each of $[y, x]$, $[y, x, x]$, $[y, x, y]$, $[y, x, x, y]$ and $[y, x, x, y, y]$.

We could continue. The simplest commutator appearing as a factor of w is $[y, x]$, and there are three of these. Suppose we collect these leftward, to a position just to the right of the three copies of y . To do this, we will need to pay “transit fees” by inserting commutators like $[[y, x, x], [y, x]]$ and others. This will result in a formula of the form $(xy)^3 = x^3y^3[y, x]^3w'$, where w' is a product of commutators of “weight” 3 and higher. This seems like quite a mess, but it is possible to do all of this in a systematic way, and to keep track of everything, and this is the Hall “commutator collection process”, which we will not pursue further.

If P has class at most 2, everything becomes much easier. In that case, the commutator $[y, x]$ is central, and so every copy of $[y, x]$ can be moved to the far right, where it will not interfere with further collection. We simply need to count how many copies of $[y, x]$ we produce as we collect the n

copies of x leftward in $(xy)^n$. The leftmost x starts in its desired position, and it need not be moved. The second x moves across one y , incurring one payment of $[y, x]$; the third x moves across two copies of y generating two additional copies of $[y, x]$; the fourth x generates three more copies of $[y, x]$, and so on. In total, therefore, we obtain $1 + 2 + \cdots + (n - 1) = (n - 1)n/2$ copies of $[y, x]$, and this establishes the formula

$$(xy)^n = x^n y^n [y, x]^{n(n-1)/2},$$

in a nilpotent group with class at most 2.

Two useful consequences of this formula are given in the following result.

4.8. Theorem. *Let P be a p -group with nilpotence class at most 2, and assume that $p > 2$. The following then hold.*

- (a) *The set $\{x \in P \mid x^p = 1\}$ is a subgroup of P .*
- (b) *If $[y, x]^p = 1$ for all $x, y \in P$, then the map $x \mapsto x^p$ is a homomorphism from P into itself.*

Proof. First, assume that $[y, x]^p = 1$ for all $x, y \in P$. Since the nilpotence class of P is at most 2, we can apply our commutator collection formula to conclude that $(xy)^p = x^p y^p [y, x]^m$, where $m = p(p - 1)/2$. Since $p \neq 2$, however, m is a multiple of p , and thus $[y, x]^m = 1$. It follows that $(xy)^p = x^p y^p$, and thus the map $x \mapsto x^p$ is a group homomorphism, proving (b).

Now (without assuming that p th powers of commutators in P are trivial) observe that since all commutators in P are central, the map $[\cdot, x]$ from P to P' is a group homomorphism for every element $x \in P$. If $y \in P$ and $y^p = 1$, therefore, we have $[y, x]^p = [y^p, x] = [1, x] = 1$ for all $x \in P$. In particular, if both $x^p = 1$ and $y^p = 1$, then commutator collection yields $(xy)^p = x^p y^p [y, x]^m = 1$, where as before, $m = p(p - 1)/2$ is a multiple of p because $p \neq 2$. The set $\{x \in P \mid x^p = 1\}$ is thus closed under multiplication, and so it is a subgroup. ■

Observe that the conclusion of Theorem 4.8(a) is equivalent to saying that $x^p = 1$ for every element $x \in \Omega_1(P)$.

Problems 4A

4A.1. Suppose that $G = AB$, where A and B are abelian subgroups. Show that $G' = [A, B]$.

4A.2. Let H , K and L be subgroups of order 2 in some group G , and observe that the set $\{[h, k, l] \mid h \in H, k \in K, l \in L\}$ contains at most one nonidentity element, and so it generates a cyclic group. Now let $G = A_5$, the

alternating group of degree 5. Show that it is possible to choose subgroups H , K and L of order 2 such that $[H, K, L] = G$.

Hint. Let $P \subseteq G$ have order 5. Choose $H, K \subseteq \mathbf{N}_G(P)$ with $H \neq K$, and choose $L \not\subseteq \mathbf{N}_G(P)$. Show that $[H, K] = P$ and observe that $\langle P, L \rangle = G$.

Note. This problem shows that $[H, K, L]$ is not necessarily generated by elements of the form $[h, k, l]$ with $h \in H$, $k \in K$ and $l \in L$.

4A.3. Say that a group Q is **quasiquaternion** if $Q = CU$, where C and U are cyclic subgroups, with $C \triangleleft Q$ and $C \cap U = \mathbf{Z}(Q)$. (Note that generalized quaternion and semidihedral groups are quasiquaternion.) Suppose that G/Z is quasiquaternion, where $Z \subseteq G' \cap \mathbf{Z}(G)$. Show that $Z = 1$.

Hint. Let \bar{A} and \bar{B} be the subgroups of $\bar{G} = G/Z$ corresponding to C and U of the definition of “quasiquaternion”. Show that $A \cap B = \mathbf{Z}(G)$ and apply Lemma 4.6.

Note. Given any group Q , consider abelian groups Z that can be isomorphically embedded in some group G in such a way that $Z \subseteq G' \cap \mathbf{Z}(G)$ and $G/Z \cong Q$. It is a fact that up to isomorphism, there is a unique largest such group Z , depending on Q ; it is called the **Schur multiplier** of Q . The homomorphic images of the Schur multiplier are all of the groups Z that satisfy our conditions. This problem asserts that quasiquaternion groups have trivial Schur multipliers. (A little more information about Schur multipliers appears in Chapter 5.)

4A.4. A p -group P is said to be **extraspecial** if $P' = \mathbf{Z}(P)$ has order p . Show that if P is extraspecial, then $P/\mathbf{Z}(P)$ is elementary abelian, or equivalently, $\mathbf{Z}(P) = P' = \Phi(P)$.

Note. Nonabelian p -groups of order p^3 are extraspecial.

4A.5. Let P be an extraspecial p -group and let $x, y \in P$ with $xy \neq yx$. Let $U = \langle x, y \rangle$ and $V = \mathbf{C}_P(U)$.

- (a) Show that $|P : \mathbf{C}_P(x)| = p$.
- (b) Show that $|U| = p^3$.
- (c) Show that $|P : V| = p^2$.
- (d) If $P > U$, show that $\mathbf{Z}(V) = \mathbf{Z}(P)$ and that V is extraspecial.
- (e) Show that $|P : \mathbf{Z}(P)| = p^{2e}$ for some integer e .

Hint. Use induction on $|P|$ for e .

Note. For every odd integer $n > 1$ and every prime p , there are exactly two isomorphism types of extraspecial p -groups of order p^n . If $p \neq 2$, these groups can be distinguished by the fact that one of them has exponent p and the other has exponent p^2 .

4A.6. Let P be a p -group having maximal class, and let $N \triangleleft P$, where $|N : P| \geq p^2$. Show that N is one of the terms of the lower central series for P , and in particular, N is the only normal subgroup of G having order $|N|$.

4A.7. Fix a prime p and let A be the external direct product of p copies of a cyclic group C of order p^n with $n > 0$. View the elements of A as p -tuples of the form (c_1, c_2, \dots, c_p) with $c_i \in C$. Let $U = \langle u \rangle$ be cyclic of order p , and let U act on A by cycling the components. In other words,

$$(c_1, c_2, \dots, c_{p-1}, c_p)^u = (c_p, c_1, c_2, \dots, c_{p-1}).$$

Finally, let $P = A \rtimes U$ be the semidirect product, and view A and U as subgroups of P . Show that the maximum of the orders of the elements of P is exactly p^{n+1} .

Note. Of course, P is just the regular wreath product $P = C \wr U$. Taking $n = 1$, we get an example where $\Omega_1(P)$ does not have exponent p .

4A.8. Assume the notation of Problem 4A.7 with $n > 0$.

- Show that $C_A(U) = \mathbf{Z}(P)$ is the set of p -tuples in A such that all components are equal.
- Show that $[A, U] = P'$ is the set of p -tuples in A such that the product of the components (computed in C) is the identity.
- Show $|\mathbf{Z}(P'U)| = p$.
- If $n = 1$, show that P has maximal class, and that in any case, $P'U$ has maximal class.

4A.9. Let $G = NA$, where $N \triangleleft G$ and $A \subseteq G$, and let M be the final term in the series $N \supseteq [N, A] \supseteq [N, A, A] \supseteq [N, A, A, A] \supseteq \dots$.

- Show that $A \triangleleft\triangleleft G$ if and only if $M \subseteq A$.
- If $M \subseteq A$, show that $M \subseteq A^\infty$.

4A.10. Let P be a p -group with $|P : \mathbf{Z}(P)| \leq p^n$. Show that

$$|P'| \leq p^{n(n-1)/2}.$$

Hint. Induct on n . If P is nonabelian, choose Q so that $\mathbf{Z}(P) \subseteq Q \subseteq P$ with $|P : Q| = p$. Get a bound on $|Q'|$ and then apply Lemma 4.6 to the group P/Q' . Note that $(P/Q')' = P'/Q'$.

Note. If the center of a group has small index, then the group is in some sense “nearly abelian”, and so it should be no surprise that the derived subgroup is not too big.

4A.11. Let $G = A \wr H$ be the regular wreath product of an abelian group A with an arbitrary finite group H , and view the base subgroup B as the group of functions $f : H \rightarrow A$ with pointwise multiplication. Let $K \subseteq H$. Show that $[B, K]$ is exactly the set of functions $f \in B$ with the property that the product of the values of f over each left coset of K in H is the identity. Deduce that $|[B, K]| = |A|^{|H|-|H:K|}$.

Hint. The action of H on B is given by $f^h(x) = f(xh^{-1})$ for $h \in H$.

4A.12. Given a finite group H , let $T(H)$ denote the set of subgroups T of H maximal with the property that T is abelian and can be generated by two elements. Let $G = A \wr H$ as in Problem 4A.11, where A is abelian, and let B be the base group.

- (a) Show that if $x, y \in G$ and $[x, y] \in B$, then $[x, y] \in [B, T]$ for some member $T \in T(H)$.
- (b) Show that if

$$\frac{1}{|A|} > \sum_{T \in T(H)} \left(\frac{1}{|A|} \right)^{|H:T|},$$

then $G' \cap B$ contains elements that are not commutators in G .

- (c) If H is not an abelian group that can be generated by two elements, show that there exists some number m such that the inequality of (b) holds whenever $|A| > m$. In particular, show that we can take $m = 3$ if $H = D_8$.

4A.13. Let G be nilpotent group with class $m > 1$, and let $a \in G$. Show that the nilpotence class of the subgroup $H = G' \langle a \rangle$ is less than m .

4B

An amazing commutator formula is the Hall-Witt identity:

$$[x, y^{-1}, z]^y [y, z^{-1}x]^z [z, x^{-1}, y]^x = 1,$$

which holds for every three elements of every group. Its proof, which proceeds by expansion and cancellation, is completely elementary and utterly routine. It is a computation that is fun to carry out, however, and we urge the reader to do so. One can think of the Hall-Witt formula as a kind of three-variable version of the much more elementary two-variable identity, $[x, y][y, x] = 1$. This observation hints at the possibility that a corresponding four-variable formula might exist, but if there is such a four-variable identity, it has yet to be discovered.

We digress briefly to mention that the Hall-Witt identity is analogous to the somewhat simpler Jacobi identity for additive commutators in a ring.

(We are assuming associativity of multiplication, of course.) If $x, y \in R$, where R is a ring, the additive commutator of x and y is $xy - yx$, which is zero precisely when x and y commute. Unfortunately, the standard notation for the additive commutator of x and y in a ring is exactly the same as the notation for group commutators: $[x, y]$. But we will not refer to additive commutators outside of this paragraph, and so we hope that this ambiguity will not cause any confusion. The Jacobi identity asserts that $[x, y, z] + [y, z, x] + [z, x, y] = 0$ for all $x, y, z \in R$, where R is a ring, and where as with groups, the triple commutators are defined by left association. We mention that a (nonassociative) ring L with multiplication $x \cdot y$ is a **Lie ring** if $x \cdot x = 0$ for all $x \in L$ and the Jacobi identity $(x \cdot y) \cdot z + (y \cdot z) \cdot x + (z \cdot x) \cdot y = 0$ holds for all $x, y, z \in L$. In particular, every associative ring is a Lie ring with respect to the multiplication $x \cdot y = [x, y]$. In fact, Lie rings provide a powerful tool for the study of p -groups, but we will say no more about that here.

Our principal applications of the Hall-Witt identity rely on the following lemma and its corollary, both of which are referred to as the “three-subgroups lemma.”

4.9. Lemma. *Let X, Y and Z be subgroups of an arbitrary group G , and suppose that $[X, Y, Z] = 1$ and $[Y, Z, X] = 1$. Then $[Z, X, Y] = 1$.*

Proof. We want to show that $[[Z, X], Y] = 1$, or equivalently, that every element of the group $[Z, X]$ commutes with every element of Y . For this purpose, we show that all commutators $[z, x]$ for $z \in Z$ and $x \in X$ centralize each element $y \in Y$. This is sufficient because $C_G(y)$ is a subgroup of G , and so if it contains all of the commutators $[z, x]$, then it contains the subgroup $[Z, X]$ generated by these commutators. It is, therefore, enough to show that $[z, x, y] = 1$, for all $x \in X, y \in Y$ and $z \in Z$. (But recall that in general, these commutators do not generate $[Z, X, Y]$.) Equivalently, it suffices to show that $[z, x^{-1}, y] = 1$ for all x, y and z in X, Y and Z , respectively.

Now $[x, y^{-1}] \in [X, Y]$, and so $[x, y^{-1}, z] \in [X, Y, Z] = 1$, and we have $[x, y^{-1}, z]^y = 1$. Similarly, $[y, z^{-1}, x]^z = 1$, and thus by the Hall-Witt identity, $[z, x^{-1}, y]^x = 1$. Thus $[z, x^{-1}, y] = 1$, as wanted. ■

4.10. Corollary. *Let N be a normal subgroup of a group G , and let $X, Y, Z \subseteq G$ be arbitrary subgroups. If $[X, Y, Z] \subseteq N$ and $[Y, Z, X] \subseteq N$, then $[Z, X, Y] \subseteq N$.*

Proof. Let $\overline{G} = G/N$ and follow the standard “bar convention”. By Lemma 4.2, we have $[\overline{H}, \overline{K}] = [\overline{H}, \overline{K}]$ for all subgroups H and K of G . Then

$$[\overline{X}, \overline{Y}, \overline{Z}] = [[\overline{X}, \overline{Y}], \overline{Z}] = [[\overline{X}, \overline{Y}], \overline{Z}] = [\overline{X}, \overline{Y}, \overline{Z}] = 1$$

and similarly, $[\overline{Y}, \overline{Z}, \overline{X}] = 1$. By Lemma 4.9 then, $1 = [\overline{Z}, \overline{X}, \overline{Y}] = \overline{[Z, X, Y]}$ and thus $[Z, X, Y] \subseteq N$. ■

An appeal to the three-subgroups lemma in a proof often makes it possible to avoid tedious and messy elementwise commutator calculations. Unfortunately, it is not always easy to see how to apply this very useful tool. We give a number of applications here and in what follows, and these should provide plenty of practice.

First, we obtain some additional information about the lower central series.

4.11. Theorem. *As usual, write G^n to denote the n th term of the lower central series of a group G . Then $[G^i, G^j] \subseteq G^{i+j}$ for integers $i, j \geq 1$.*

Proof. We proceed by induction on j , which is the superscript on the right in the commutator $[G^i, G^j]$. Since $G^1 = G$, we see that if $j = 1$, the formula we need is $[G^i, G] \subseteq G^{i+1}$, and this is valid since by definition, $G^{i+1} = [G^i, G]$. We can assume, therefore, that $j > 1$, and so we can write $G^j = [G^{j-1}, G]$. Then

$$[G^i, G^j] = [G^j, G^i] = [G^{j-1}, G, G^i],$$

and to show that this triple commutator is contained in the normal subgroup G^{i+j} , it suffices by the three-subgroups lemma (Corollary 4.10) to show that

$$[G, G^i, G^{j-1}] \subseteq G^{i+j} \quad \text{and} \quad [G^i, G^{j-1}, G] \subseteq G^{i+j}.$$

We have

$$[G, G^i, G^{j-1}] = [G^i, G, G^{j-1}] = [G^{i+1}, G^{j-1}] \subseteq G^{(i+1)+(j-1)} = G^{i+j},$$

where the containment is valid by the inductive hypothesis. Also,

$$[G^i, G^{j-1}, G] \subseteq [G^{i+j-1}, G] = G^{i+j},$$

where here too, the containment follows from the inductive hypothesis. This completes the proof. ■

Suppose we consider commutators of n copies of G that are not necessarily left associated. For example, if $n = 8$, we might have something like $[[[G, G], [G, G, G]], [[G, G], G]]$. (We refer to such an object as a commutator of **weight** n .) The following result shows that the left-associated weight n commutator of copies of G contains every other such weight n commutator. (Of course, the left associated weight n commutator is exactly G^n , the n th term of the lower central series.)

4.12. Corollary. *Let G be a group. Then every weight n commutator of copies of G is contained in G^n .*

Proof. We proceed by induction on n . The only weight 1 commutator is G itself, and so there is nothing to prove in this case. An arbitrary weight n commutator with $n > 1$ has the form $[X, Y]$, where X is a weight i commutator, Y is a weight j commutator and $i + j = n$. Since $i < n$ and $j < n$, the inductive hypothesis yields $X \subseteq G^i$ and $Y \subseteq G^j$, and thus $[X, Y] \subseteq [G^i, G^j] \subseteq G^{i+j} = G^n$ by Theorem 4.11. ■

Consider the terms $G^{(r)}$ of the derived series of G . We see that $G' = [G, G]$ is a weight 2 commutator, $G'' = [G', G'] = [[G, G], [G, G]]$ is a weight 4 commutator, and $G''' = [G'', G'']$ is a weight 8 commutator. In general, $G^{(r)}$ is a weight 2^r commutator for all $r \geq 0$, and this yields the following.

4.13. Corollary. *We have $G^{(r)} \subseteq G^{2^r}$ for all groups G and integers $r \geq 0$. Also, if G is nilpotent of class m , then the derived length of G is at most $1 + \log_2(m)$.*

Proof. Since $G^{(r)}$ is a weight 2^r commutator, the first assertion is immediate from Corollary 4.12. Now assume that G is nilpotent of class m , and let d be its derived length, so that $G^{(d)} = 1$ and d is the smallest integer with this property. We have

$$G^{2^{d-1}} \supseteq G^{(d-1)} > 1 = G^{m+1},$$

and so $2^{d-1} < m + 1$. Then $2^{d-1} \leq m$, and hence $d - 1 \leq \log_2(m)$. ■

Next, we explore some connections between the conjugacy class sizes and the nilpotence class of a nilpotent group G . Suppose we know the number m of different sizes of conjugacy classes in G . If $m = 1$, for example, then since the size of the class of the identity of G is 1, it follows that all classes of G have size 1, and so G is abelian. (Of course, we did not use the assumption that G is nilpotent here.) This suggests the (still unresolved) question of how the number m of conjugacy class sizes of G affects the structure of G . In particular, it would be interesting to know if the derived length of G , or perhaps even the nilpotence class of G , is bounded by some function of m .

After many years without progress on these questions, it was proved by K. Ishikawa that if $m = 2$, then G has nilpotence class at most 3. (In this case too, it is not really necessary to assume that G is nilpotent; a result of N. Ito shows that a finite group with just two class sizes is necessarily nilpotent.) More recently, A. Mann proved a stronger result with an easier proof, and we present that next.

Given a finite group G with class sizes $1 = n_1 < n_2 < \cdots < n_m$, we write $\mathbf{M}(G)$ to denote the subgroup of G generated by all elements lying in conjugacy classes of size at most n_2 . (We will use this notation for the

remainder of this section.) Note that $\mathbf{M}(G) = G$ if $m = 2$, and thus the following result contains Ishikawa's theorem.

4.14. Theorem (Mann). *If G is a finite nilpotent group, then the nilpotence class of $\mathbf{M}(G)$ is at most 3.*

Actually, we can replace the hypothesis that G is nilpotent in Theorem 4.14 by a much weaker one: that G has a self-centralizing normal subgroup. (By this, we mean a subgroup $A \triangleleft G$ such that $A = \mathbf{C}_G(A)$. Observe that such a subgroup is automatically abelian.)

4.15. Theorem. *Suppose that a finite group G contains a self-centralizing normal subgroup. Then $\mathbf{M}(G)$ is nilpotent, and its nilpotence class is at most 3.*

Recall that a nilpotent group G always has a self-centralizing normal subgroup, and so Theorem 4.14 is immediate from Theorem 4.15. (The existence of self-centralizing normal subgroups in nilpotent groups is part of Problem ID.10, but nevertheless, we give the easy proof here.)

4.16. Lemma. *Let G be a finite nilpotent group, and let A be maximal among normal abelian subgroups of G . Then $A = \mathbf{C}_G(A)$, and hence every nilpotent group contains a self-centralizing normal subgroup.*

Proof. Write $G = \mathbf{C}_G(A)$. Then $A \subseteq C$, and we assume that this containment is proper. Since $A \triangleleft G$, we have $C \triangleleft G$, and thus we can choose a subgroup $B \subseteq C$ such that B/A is minimal normal in G/A . Since G/A is nilpotent, it follows that $B/A \subseteq \mathbf{Z}(G/A)$, and thus B/A has prime order. In particular, B/A is cyclic, and since $B \subseteq G = \mathbf{C}_G(A)$, it follows that $A \subseteq \mathbf{Z}(B)$. We conclude that B is abelian, and since $B \triangleleft G$, this contradicts the choice of A . ■

The key ingredient in the proof of Theorem 4.15 is the following.

4.17. Lemma. *Let K be an abelian normal subgroup of a finite group G , and let $x \in G$ be noncentral. Then $|\mathbf{C}_G(x)| < |\mathbf{C}_G(y)|$, where $y = [k, x]$ and $k \in K$ is arbitrary.*

Proof. Observe that $y \in [K, G] \subseteq K$. If $y = 1$, then $\mathbf{C}_G(y) = G > \mathbf{C}_G(x)$, and there is nothing further to prove, so we assume that $y \neq 1$. Both x and y lie in the subgroup $H = K\mathbf{C}_G(x)$, and of course, $\mathbf{C}_H(x) = \mathbf{C}_G(x)$ and $\mathbf{C}_H(y) \subseteq \mathbf{C}_G(y)$. It suffices, therefore, to prove that $|\mathbf{C}_H(x)| < |\mathbf{C}_H(y)|$.

Now let $\theta : K \rightarrow K$ be the map defined by $\theta(t) = [t, x]$. For $s, t \in K$, we have

$$\theta(st) = [st, x] = [s, x]^t[t, x] = [s, x][t, x] = \theta(s)\theta(t),$$

where the third equality holds because both t and $[s, x]$ lie in the abelian group K . Thus θ is a homomorphism, and $\theta(K)$ is a subgroup, and we have

$$|\theta(K)| = |K : \ker(\theta)| = |K : K \cap \mathbf{C}_H(x)| = |H : \mathbf{C}_H(x)|.$$

We argue next that each of the subgroups K and $\mathbf{C}_G(x)$ normalizes $\theta(K)$, and thus $\theta(K) \triangleleft K\mathbf{C}_G(x) = H$. Certainly, $K \subseteq \mathbf{N}_G(\theta(K))$ since $\theta(K) \subseteq K$ and K is abelian. Also, since $\theta(K)$ is uniquely determined by the normal subgroup K and the element x , we see that $\mathbf{C}_G(x) \subseteq \mathbf{N}_G(\theta(K))$. Now $\theta(K) \triangleleft H$, and y is a nonidentity element of $\theta(K)$, and thus the entire H -conjugacy class Y of y consists of nonidentity elements of $\theta(K)$. Then $|H : \mathbf{C}_H(y)| = |Y| < |\theta(K)| = |H : \mathbf{C}_H(x)|$, as required. ■

4.18. Corollary. *Let K be an abelian normal subgroup of an arbitrary finite group G , and write $M = \mathbf{M}(G)$. Then $[K, M] \subseteq \mathbf{Z}(G)$.*

Proof. Write $\overline{G} = G/\mathbf{Z}(G)$. It suffices to show that $[\overline{K}, \overline{M}] = 1$, and for this purpose, it is enough to check that \overline{x} centralizes \overline{K} for all elements x in some generating set for M . It suffices, therefore, to observe that $[k, x] \in \mathbf{Z}(G)$ for all $k \in K$, where x lies in a conjugacy class of size 1 or n_2 in G . Of course, if $x \in \mathbf{Z}(G)$, there is nothing to prove, and if x lies in a class of size n_2 , then by Lemma 4.17, the element $[k, x]$ lies in a smaller class, and hence $[k, x] \in \mathbf{Z}(G)$, as required. ■

Proof of Theorem 4.15. Let $K \triangleleft G$ be self-centralizing, and write $M = \mathbf{M}(G)$. By Corollary 4.18, we have $[K, M] \subseteq \mathbf{Z}(G)$, and thus $[K, M, M] = 1$ and $[M, K, M] = 1$. By the three-subgroups lemma, $[M, M, K] = 1$, and thus $[M, M] \subseteq \mathbf{C}_G(K) = K$. Then $M^4 = [M, M, M, M] \subseteq [K, M, M] = 1$, and it follows that M is nilpotent with class at most 3. ■

We clearly cannot drop the assumption in Theorem 4.15 that G contains a self-centralizing normal subgroup since, for example, if G is nonabelian and simple, then $\mathbf{M}(G) = G$ is certainly not nilpotent. We do, however, obtain the following very general result.

4.19. Theorem. *Let G be a finite group, and write $F = \mathbf{F}(M)$, where $M = \mathbf{M}(G)$. Then the nilpotence class of F is at most 4.*

Proof. Let n be the nilpotence class of F , so that $F^n > 1$ and $F^{n+1} = 1$. Assuming, as we may, that $n \geq 3$, consider the characteristic subgroup F^{n-2} of G . If this subgroup is abelian, then by Corollary 4.18, we have $[F^{n-2}, M] \subseteq \mathbf{Z}(G)$, and thus $F^n = [F^{n-2}, F, F] \subseteq [F^{n-2}, M, F] = 1$, which is a contradiction. We conclude that F^{n-2} is nonabelian, and therefore $1 < [F^{n-2}, F^{n-2}] \subseteq F^{2n-4}$ by Theorem 4.11. But $F^{n+1} = 1$, and thus $2n - 4 < n + 1$. This yields $n \leq 4$, as wanted. ■

Problems 4B

4B.1. Let G be nilpotent of class exceeding 2. Show that G has a characteristic abelian subgroup that is not central.

4B.2. Let G be nilpotent. Show that G has a characteristic subgroup K such that $K \supseteq \mathbf{C}_G(K)$ and the nilpotence class of K is at most 2.

Hint. Use Problem 4B.1.

4B.3. Let $\{Z_j \mid j \geq 1\}$ be the upper central series for an arbitrary group G . Show that $[G^i, Z_j] \subseteq Z_{j-i}$ for all $i > 0$ and all j . In particular, $[G^i, Z_i] = 1$ for $i > 0$.

4B.4. Let $X, Y \subseteq G$ be arbitrary subgroups, and suppose that Y centralizes $[X, Y]$.

(a) Prove that Y' centralizes X .

(b) Now assume that $X \triangleleft G$. Show that $[X, Y]$ is abelian.

4B.5. Let G be supersolvable. Show that $\mathbf{M}(G)$ is nilpotent with class at most 3.

4C

Let A act on G via automorphisms. Since A and G can be viewed as subgroups of the semidirect product $\Gamma = G \rtimes A$, the commutator $[G, A]$ can be computed as a subgroup of Γ . But $G \triangleleft \Gamma$, and so $[G, A] \subseteq G$, and in fact it is possible (and often convenient) to think of $[G, A]$ as being computed entirely within G , thereby rendering the semidirect product irrelevant. To do this, observe that if $g \in G$ and $a \in A$, then $[g, a] = g^{-1}a^{-1}ga = g^{-1}g^a$, where we can view g^a either as the result of conjugating g by a in Γ , or alternatively, as the result of applying a to g in the original action. The commutator $[G, A]$, therefore, is the subgroup $\langle g^{-1}g^a \mid g \in G, a \in A \rangle$, and this would make sense even if we did not know about semidirect products. Nevertheless, to prove facts about $[G, A]$ and related objects, we will appeal to semidirect products when it is convenient to do so, and in particular, we will apply the three-subgroups lemma to subgroups of the semidirect product.

We can apply Lemma 4.1 (in the semidirect product) to deduce that $[G, A] \triangleleft G$. Also A normalizes $[G, A]$ in $G \rtimes A$, which means that $[G, A]$ is invariant under conjugation by elements of A , or equivalently, it is invariant under the original action of A on G . In general, if $H \subseteq G$ is an arbitrary A -invariant subgroup, we have a natural action of A on H , and sometimes in this context, we say that H **admits** the action of A . In particular, since

$[G, A]$ admits the action of A , we can compute $[G, A, A]$, which is normal in $[G, A]$, but not necessarily in G . (It is, of course, *subnormal* in G .) Also, $[G, A, A]$ admits A , and thus we can compute $[G, A, A, A]$, and we can continue like this. All of these repeated commutators, of course, admit A and are subnormal in G .

Recall that if A acts via automorphisms on G and $H \subseteq G$ is A -invariant, then A permutes the set of right cosets of H in G and also the set of left cosets of H in G . In particular, if $H \triangleleft G$, we have an action of A on G/H , and it is easy to see that this is an action via automorphisms. (This is sometimes called the **induced action** of A on G/H .) For $g \in G$ and $a \in A$, we have $(gH)^a = g^aH$, and so if we write $\overline{G} = G/H$ we have $(\overline{g})^a = \overline{g^a}$, and hence

$$\overline{[g, a]} = \overline{g^{-1}g^a} = (\overline{g^{-1}})(\overline{g^a}) = (\overline{g})^{-1}(\overline{g})^a = \overline{[g, a]}.$$

It follows that $\overline{[G, A]} = [\overline{G}, A]$.

The following characterization of $[G, A]$ is sometimes useful.

4.20. Lemma. *Let A act via automorphisms on G , where A and G are groups. Then $[G, A]$ is the unique smallest A -invariant normal subgroup of G such that the induced action of A on the factor group is trivial.*

Proof. Suppose that $N \triangleleft G$, where N is A -invariant, and write $\overline{G} = G/N$. Then A acts trivially on G/N if and only if $1 = [\overline{G}, A]$, which by the previous computation is equivalent to $1 = \overline{[G, A]}$. This, of course, is the same as $[G, A] \subseteq N$, and the result is now immediate. ■

4.21. Corollary. *Let A act via automorphisms on G , where A and G are groups, and let $H \subseteq G$. Then the following are equivalent.*

- (a) *Every right coset of H in G is an A -invariant subset.*
- (b) *Every left coset of H in G is an A -invariant subset.*
- (c) $[G, A] \subseteq H$.

In particular, $[G, A]$ is the unique smallest subgroup of G with the property that all of its right cosets are A -invariant, and similarly if “left” replaces “right”.

Proof. First, observe that if X is a subset of G and we write $X^{-1} = \{x^{-1} \mid x \in X\}$, then the map $X \mapsto X^{-1}$ takes the right cosets of H to the left cosets of H and *vice versa*. It follows that an automorphism of G fixes all right cosets of H if and only if it fixes all left cosets of H . We see, therefore, that (a) and (b) are equivalent.

Now assume (b), so that every left coset of H is A -invariant. Then for $g \in G$ and $a \in A$, we have $g^a \in (gH)^a = gH$, and so $[g, a] = g^{-1}g^a \in H$ and (c) follows.

Finally, assume (c), so that $[G, A] \subseteq H$. Each right coset of H in G , therefore, is a union of right cosets of $[G, A]$ in G . But all cosets of $[G, A]$ in G are A -invariant by Lemma 4.20, and so unions of such cosets are also A -invariant, and (a) follows. ■

Recall that an action of a group A on a set Ω is faithful if the identity of A is the only element that fixes every point. In general, the kernel of an arbitrary action of a group A is the (necessarily normal) subgroup B of A consisting of the elements of A that act trivially. In this situation, all elements of each coset Ba of B in A induce the same permutation on Ω , and so we have a well defined action of $\bar{A} = A/B$ on Ω , where $\alpha \cdot \bar{a} = \alpha \cdot a$. This action of A/B is clearly faithful.

Now suppose that A acts on G via automorphisms. Working in the semidirect product $G \rtimes A$, we see that the kernel of the action of G on A is $\mathbf{C}_A(G)$. (As we remarked previously, it is common to write $\mathbf{C}_A(G)$ to denote the kernel of the action of A on G even if we do not explicitly construct the semidirect product.) This kernel is the largest subgroup $B \subseteq A$ such that $[G, B] = 1$. If $B = \mathbf{C}_A(G)$, then $B \triangleleft A$, and writing $\bar{A} = A/B$ as before, we see that the natural action of \bar{A} on G is given by $g^{\bar{a}} = g^a$ for $g \in G$ and $a \in A$, and it follows that a subgroup $H \subseteq G$ is A -invariant if and only if it is \bar{A} -invariant. (In other words H admits A if and only if it admits \bar{A} .) Also, $[g, \bar{a}] = [g, a]$ for $g \in G$ and $a \in A$, and so if H admits A and \bar{A} , we have $[H, A] = [H, \bar{A}]$.

What can we say about the structure of a group A if we know that it acts via automorphisms on some group G in such a way that $[G, A, \dots, A] = 1$, where there are (say) m copies of A in this commutator? The answer is that we can say precisely nothing. This is because an arbitrary group A can act trivially on G , in which case $[G, A] = 1$. More generally, if B is the kernel of the action of A on G , then B and G cannot “see” each other, and so the fact that $[G, A, \dots, A] = 1$ tells us nothing about B . To draw a conclusion about the structure of A from some assumption about how G sees the action of A , we must therefore assume that the action is faithful.

To facilitate the discussion, we introduce some (nonstandard) notation. We write $[G, A, \dots, A]_m$ to denote the commutator with exactly m copies of A . Then $[G, A, \dots, A]_1$ is simply $[G, A]$ and in general $[[G, A], A, \dots, A]_m = [G, A, \dots, A]_{m+1}$.

4.22. Theorem. *Let A and G be groups. Suppose that A acts faithfully on G via automorphisms, and assume that $[G, A, \dots, A]_m = 1$. Then A is solvable, and its derived length is at most $m - 1$.*

Proof. We begin by reformulating the result in such a way that we need not assume that the action is faithful. In the general case, we cannot hope

to prove that A is solvable, but we show by induction on m that $A^{(m-1)} \subseteq \mathbf{C}_A(G)$, where we recall that $\mathbf{C}_A(G)$ is the kernel of the action. In the original situation, where A acts faithfully, we have $\mathbf{C}_A(G) = 1$, and it will follow that $A^{(m-1)} = 1$, and so A is solvable with derived length at most $m - 1$, as required.

If $m = 1$, then $[G, A] = 1$, and thus $A = \mathbf{C}_G(A)$ and there is nothing more to prove. Assume then, that $m \geq 2$, and let $H = [G, A]$, so that H admits A and $[H, A, \dots, A]_{m-1} = [G, A, \dots, A]_m = 1$. By the inductive hypothesis applied to the action of A on H , therefore, we have $A^{(m-2)} \subseteq \mathbf{C}_A(H)$, and thus $1 = [H, A^{(m-2)}] = [G, A, A^{(m-2)}]$. Since $A \supseteq A^{(m-2)}$, it follows that $[G, A^{(m-2)}, A^{(m-2)}] = 1$, and thus also $[A^{(m-2)}, G, A^{(m-2)}] = 1$ since interchanging the first two entries in a multiple commutator of subgroups has no effect. The three-subgroups lemma now yields

$$[A^{(m-2)}, A^{(m-2)}, G] = 1,$$

and since by definition,

$$A^{(m-1)} = [A^{(m-2)}, A^{(m-2)}],$$

we have $[A^{(m-1)}, G] = 1$. Thus $A^{(m-1)} \subseteq \mathbf{C}_A(G)$, as wanted. ■

When $m > 2$, the step in the proof of Theorem 4.22 where A is replaced by $A^{(m-2)}$ throws away information, and this suggests that perhaps more is true than we proved. In fact more is true: P. Hall showed that under the hypotheses of our theorem, A is actually nilpotent, and not merely solvable. Also, the nilpotence class of A is at most $m(m-1)/2$. Recall that by Corollary 4.13, the derived length of a nilpotent group is logarithmically bounded in terms of its nilpotence class, and therefore it follows by Hall's theorem that the linear bound on the derived length of A that we established in Theorem 4.22 is too weak; it is of the "wrong" order of magnitude.

If $m = 2$, then $A^{(m-2)} = A^{(0)} = A$, and we lose nothing in the replacement step of the previous proof. In this case, Hall's result coincides with Theorem 4.22 since a nontrivial group is solvable with derived length 1 if and only if it is abelian, which is exactly when it is nilpotent with class 1. We list this case as a separate corollary.

4.23. Corollary. *Let A and G be groups. Suppose that A acts faithfully on G via automorphisms and that $[G, A, A] = 1$. Then A is abelian.*

Proof. This is just the case $m = 2$ of Theorem 4.22. ■

Without using additional machinery, it seems to be difficult to establish Hall's upper bound on the nilpotence class of A . But it is not too hard to show that A is nilpotent in the situation we have been discussing, and the proof offers more opportunities for using the three-subgroups lemma.

4.24. Theorem. *Let A and G be finite groups. Suppose that A acts faithfully via automorphisms on G , and assume that $[G, A, \dots, A] = 1$. Then A is nilpotent.*

Proof. As before, we drop the assumption that A acts faithfully. We prove by induction on $|G|$ that in general, the last term A^∞ of the lower central series of A acts trivially on G . Once this is established, we see that if the action of A is faithful, then $A^\infty = 1$, and hence A is nilpotent.

Since we can assume that $G > 1$ and we know that $[G, A, \dots, A] = 1$, it follows that $[G, A] < G$. Also, $[G, A]$ admits the action of A and $[[G, A], A, \dots, A] = 1$. By the inductive hypothesis, therefore, A^∞ acts trivially on $[G, A]$, and hence $[G, A, A^\infty] = 1$, or equivalently, $[A, G, A^\infty] = 1$. Our goal will be to show that $[G, A^\infty, A] = 1$ since, if we can accomplish that, the three-subgroups lemma will yield $[A^\infty, A, G] = 1$. But $[A^\infty, A] = A^\infty$ because A^∞ is the last term of the lower central series of A , and it will follow that $[A^\infty, G] = 1$. The proof will then be complete.

Our strategy for showing that $[G, A^\infty, A] = 1$ is to find a nontrivial normal subgroup C of G on which A acts trivially. Once we have found C , we can apply the inductive hypothesis to the induced action of A on $\overline{G} = G/C$. (This is valid since we have $[\overline{G}, A, \dots, A] = \overline{[G, A, \dots, A]} = 1$.) By the inductive hypothesis, $1 = [\overline{G}, A^\infty] = \overline{[G, A^\infty]}$, and so $[G, A^\infty] \subseteq C$. Since we are assuming that A acts trivially on C , this yields $[G, A^\infty, A] = 1$, which is what we want.

We can assume that $[G, A^\infty] > 1$, or else there is nothing to prove. Take $C = C_{[G, A^\infty]}(A)$, so that A certainly acts trivially on C , as required. To see that $C > 1$, observe that $[[G, A^\infty], A, \dots, A] = 1$, and thus if we start with the nontrivial group $[G, A^\infty]$ and repeatedly compute commutators with A , we get a sequence of subgroups of $[G, A^\infty]$ terminating at the identity. The last nonidentity term in this sequence, therefore, is centralized by A , and this shows that $C > 1$, as required.

To complete the proof now, it suffices to show that $C \triangleleft G$, and our argument for this involves two further applications of the three-subgroups lemma. First, we argue that $[G, A^\infty]$ centralizes $[G, A]$. We have already mentioned that A^∞ acts trivially on $[G, A]$, so that $[[G, A], A^\infty] = 1$, and thus we have $[[G, A], A^\infty, G] = 1$. Also, $[G, A] \triangleleft G$, and thus $[G, [G, A]] \subseteq [G, A]$, and we have $[G, [G, A], A^\infty] \subseteq [[G, A], A^\infty] = 1$. Now we apply the three-subgroups lemma to deduce that $[A^\infty, G, [G, A]] = 1$, and thus $[G, A]$ centralizes $[A^\infty, G] = [G, A^\infty]$, as claimed. In particular, since $C \subseteq [G, A^\infty]$, we have $[G, A, C] = 1$. Also, of course, $[A, C, G] = 1$ since A centralizes C . By the three-subgroups lemma, once again, we have $[G, G, A] = 1$, and so A centralizes $[G, G]$.

Recall now that $C \subseteq [G, A^\infty] \triangleleft G$, and thus $[C, G] \subseteq [G, A^\infty]$. We just showed, however, that A centralizes $[C, G]$, and thus $[C, G] \subseteq \mathbf{C}_{[G, A^\infty]}(A) = C$, where the equality holds by the definition of C . We have now shown that $[C, G] \subseteq C$, or equivalently, that $C \triangleleft G$, as wanted. The proof is now complete. ■

Let us continue to assume that $[G, A, \dots, A] = 1$ for some unspecified number of copies of A . We have seen that if the action is faithful, then A must be nilpotent. It is impossible, however, to draw any conclusions about the structure of G since, for example, it could be that A is trivial. But although we can say nothing about G itself, we shall see that the subgroup $[G, A]$ is under control. We begin with a special case.

4.25. Lemma. *Let A and G be groups. Suppose that A acts on G via automorphisms, and assume that $[G, A, A] = 1$. Then $[G, A]$ is abelian.*

Proof. Since $[[G, A], A] = 1$, we certainly have $[[G, A], A, G] = 1$. Also, $[G, A] \triangleleft G$, and thus $[G, [G, A], A] \subseteq [[G, A], A] = 1$. By the three-subgroups lemma, we have

$$1 = [A, G, [G, A]] = [[G, A], [G, A]] = [G, A]',$$

and so $[G, A]$ is abelian. ■

4.26. Theorem. *Let A be a p -group that acts via automorphisms on a finite group G , and suppose that $[G, A, \dots, A] = 1$. Then $[G, A]$ is a p -group.*

Proof. We proceed by induction on $|G|$. We can certainly assume that $G > 1$, and thus since $[G, A, \dots, A] = 1$, it follows that $[G, A] < G$. For convenience, write $N = [G, A]$, and observe that $N \triangleleft G$ and that N admits the action of A . Since $N < G$, the inductive hypothesis applies in N , and we deduce that $[N, A]$ is a p -group. Also, since $[N, A] \triangleleft N$, we have $[N, A] \subseteq U$, where $U = \mathbf{O}_p(N)$ is characteristic in $N \triangleleft G$, and thus $U \triangleleft G$.

Now consider the induced action of A on $\overline{G} = G/U$. Since $[N, A] \subseteq U$, we see that A acts trivially on \overline{N} . Also, $[\overline{G}, A] = [\overline{G}, A] = \overline{N}$, and thus A acts trivially on $\overline{G}/\overline{N}$. We have $[\overline{G}, A, A] = [\overline{N}, A] = 1$, and thus by Lemma 4.25, we conclude that $\overline{N} = [\overline{G}, A]$ is abelian. But $\mathbf{O}_p(\overline{N})$ is trivial, and since \overline{N} is abelian, it follows that \overline{N} is a p' -group.

Since A is a p -group and \overline{N} is a normal p' -subgroup of \overline{G} , we can apply Corollary 3.28 to the action of A on \overline{G} . That corollary tells us that “fixed points come from fixed points”, and since \overline{N} is contained in the fixed-point subgroup and every element of $\overline{G}/\overline{N}$ is A -fixed, we conclude that the whole group \overline{G} consists of fixed points. Then $1 = [\overline{G}, A] = [\overline{G}, A]$, and hence $[G, A] \subseteq U$. Since U is a p -group, we are done. ■

In the situation of Theorem 4.26, we can conclude that $[G, A]$ is nilpotent even without assuming that A is a p -group.

4.27. Theorem. *Let A and G be finite groups. Suppose that A acts via automorphisms on G , and assume that $[G, A, \dots, A] = 1$. Then $[G, A]$ is nilpotent.*

Proof. We proceed by induction on $|A|$. (Of course, if A is trivial then $[G, A] = 1$ and there is nothing to prove.) Suppose that B is an arbitrary proper subgroup of A . Then $[G, B, \dots, B] \subseteq [G, A, \dots, A] = 1$, and so by the inductive hypothesis, $[G, B]$ is nilpotent. Since $[G, B] \triangleleft G$, we have $[G, B] \subseteq \mathbf{F}(G)$, the Fitting subgroup, and thus B acts trivially on $G/\mathbf{F}(G)$.

We now know that every proper subgroup of A is contained in the kernel of the induced action of A on $G/\mathbf{F}(G)$, and so if A is generated by its proper subgroups, then this kernel must be all of A . In this case, $[G, A] \subseteq \mathbf{F}(G)$, and hence $[G, A]$ is nilpotent, as wanted. We can assume, therefore, that A is not generated by its proper subgroups. Every finite group, however, is generated by its Sylow subgroups, and thus some Sylow subgroup of A is not proper. In other words, A is a p -group for some prime p , and hence $[G, A]$ is a p -group by Theorem 4.26. In particular, $[G, A]$ is nilpotent. ■

Problems 4C

4C.1. Let A act on G via automorphisms, and suppose that

$$1 = H_0 \subseteq H_1 \subseteq \dots \subseteq H_m = G$$

is a chain of A -invariant subgroups such that each right coset of H_{i-1} in H_i is A -invariant for all i with $0 < i \leq m$. In the older literature, this situation was described by saying that A **stabilizes** the chain $\{H_i\}$. If A stabilizes a chain of subgroups in G , show that it stabilizes a chain of subnormal subgroups.

4C.2. Assume that A acts faithfully on G via automorphisms, and assume that A stabilizes a chain $\{H_i \mid 0 \leq i \leq m\}$ of *normal* subgroups of G . Show that A is nilpotent with class at most $m - 1$.

4C.3. Let A act via automorphisms on G , and suppose that $N \triangleleft G$ and that A acts trivially on N . Show that N centralizes $[G, A]$.

4D

We continue our study of commutators that arise when A acts via automorphisms on G , but now we focus on coprime actions, where $(|G|, |A|) = 1$.

The following ultimately relies on Glauberman's lemma, and that is the reason for the solvability assumption, which, as usual, is not really necessary if one is willing to appeal to the Feit-Thompson theorem.

4.28. Lemma. *Let A and G be finite groups. Let A act via automorphisms on G , and suppose that $(|G|, |A|) = 1$ and that one of A or G is solvable. Then $G = \mathbf{C}_G(A)[G, A]$.*

Proof. Write $\overline{G} = G/[G, A]$. Since fixed points come from fixed points in coprime actions (Corollary 3.28) we have $\mathbf{C}_{\overline{G}}(A) = \overline{\mathbf{C}_G(A)}$. But A acts trivially on $G/[G, A]$, and so the left side of this equation is the whole group \overline{G} . Thus

$$\overline{\mathbf{C}_G(A)[G, A]} = \overline{\mathbf{C}_G(A)} = \overline{G},$$

and it follows that $[G, A]\mathbf{C}_G(A) = G$ by the correspondence theorem. ■

To demystify this proof somewhat, we observe that what is going on here is the following. Each coset of $[G, A]$ in G is A -invariant, and so by a fairly standard Glauberman's lemma argument, each such coset contains an A -fixed element.

The following result is used frequently.

4.29. Lemma. *Let A act via automorphisms on G , where A and G are finite groups, and suppose that $(|G|, |A|) = 1$. Then $[G, A, A] = [G, A]$.*

Proof. Of course $[G, A, A] \subseteq [G, A]$, and so it suffices to prove the reverse containment. For this purpose, we show that $[g, a] \in [G, A, A]$ for all $g \in G$ and $a \in A$. The result will then follow since $[G, A]$ is generated by these commutators $[g, a]$.

Suppose first that A is solvable. Lemma 4.28 yields $G = \mathbf{C}_G(A)[G, A]$, and so if $g \in G$, we can write $g = cx$, where $c \in \mathbf{C}_G(A)$ and $x \in [G, A]$. Now let $a \in A$, and observe that $[c, a] = 1$. Then

$$[g, a] = [cx, a] = [c, a]^x [x, a] = [x, a] \in [G, A, A],$$

as wanted. This proves that the result is true if A is solvable.

Now in the general case, again let $g \in G$ and $a \in A$. Then

$$[g, a] \in [G, \langle a \rangle] = [G, \langle a \rangle, \langle a \rangle] \subseteq [G, A, A]$$

since the cyclic group $\langle a \rangle$ is certainly solvable. This completes the proof. ■

We can apply this to the situation that we studied in the previous section.

4.30. Corollary. *Let A act faithfully via automorphisms on G , where A and G are finite groups, and assume that $[G, A, \dots, A] = 1$. Then every prime divisor of $|A|$ also divides $|G|$.*

Proof. Let $P \in \text{Syl}_p(A)$ where p is a prime that does *not* divide $|G|$. Then $[G, P] = [G, P, \dots, P] = 1$, where the first equality holds by repeated application of Lemma 4.29. Since the action of A is faithful and P acts trivially, we deduce that $P = 1$, and thus p does not divide $|A|$. ■

Next, we prove the so called $P \times Q$ lemma of Thompson, and we show how it is relevant to the study of local subgroups.

4.31. Theorem (Thompson). *Let A be a finite group that acts via automorphisms on a p -group G , and suppose that $A = P \times Q$ is an internal direct product of a p -group P and a p' -group Q . Suppose that Q fixes every element of G that P fixes. Then Q acts trivially on G .*

Before we begin the proof of Thompson's theorem, we establish some easy facts about p -groups acting on p -groups.

4.32. Lemma. *Let P be a p -group that acts via automorphisms on a nontrivial p -group G . Then $[G, P] < G$ and $\mathbf{C}_G(P) > 1$.*

Proof. The semidirect product $\Gamma = G \rtimes P$ is a p -group, and hence it is nilpotent. It follows that some repeated commutator of the form $[\Gamma, \Gamma, \dots, \Gamma]$ is trivial, and thus we have $[G, P, \dots, P] = 1$. Successive commutation with P , therefore, yields a descending sequence of subgroups starting with $G > 1$ and ending with 1. Thus $[G, P] < G$, as wanted. Also, if H is the last nonidentity group in this sequence, then $[H, P] = 1$, and so $1 < H \subseteq \mathbf{C}_G(P)$. ■

Assuming that the p -group G is nontrivial in the situation of the $P \times Q$ lemma, it follows by Lemma 4.32 that $\mathbf{C}_G(P) > 1$. By hypothesis, however, $\mathbf{C}_G(P) \subseteq \mathbf{C}_G(Q)$, and therefore Q has at least some nontrivial fixed points in G . What we need, however, is that Q fixes *every* element of G , and the proof of this, while not hard, is a little more subtle; it gives us another opportunity to use the three-subgroups lemma.

Proof of Theorem 4.31. We can assume that $G > 1$, and we proceed by induction on $|G|$. We have $[G, P] < G$ by Lemma 4.32. Also, $[G, P]$ is A -invariant since both G and P are normalized by A in the semidirect product $G \rtimes A$. The hypothesis that Q centralizes every element of G centralized by P is inherited by the action of A on $[G, P]$, and so the inductive hypothesis applies to this action. We conclude that Q acts trivially on $[G, P]$, and hence $[G, P, Q] = 1$. Also, $[P, Q, G] = 1$ since P and Q centralize each other in A . It follows by the three-subgroups lemma that $[Q, G, P] = 1$, and thus P acts trivially on $[Q, G] = [G, Q]$. By hypothesis, Q acts trivially on this subgroup too, and so $[G, Q, Q] = 1$. Finally, since Q is a p' -group and G is

a p -group, we have $[G, Q, Q] = [G, Q]$ by Lemma 4.29, and so $[G, Q] = 1$, as required. ■

As an application of the $P \times Q$ lemma, we prove the following “local to global” result for p -solvable groups. (Recall from Section 2C that if p is a prime, a subgroup $H \subseteq G$ is said to be p -local in G if $H = \mathbf{N}_G(P)$, for some nontrivial p -subgroup P of G .)

4.33. Theorem. *Let G be a finite p -solvable group for some prime p . Then $\mathbf{O}_{p'}(H) \subseteq \mathbf{O}_{p'}(G)$ for every p -local subgroup $H \subseteq G$.*

Proof. Let $Q = \mathbf{O}_{p'}(H)$, where H is p -local in G . First, we consider the case where $\mathbf{O}_{p'}(G) = 1$, and where our goal, therefore, is to show that $Q = 1$. Since H is p -local, we can write $H = \mathbf{N}_G(P)$ for some p -subgroup $P \subseteq G$, and we observe that both P and Q are normal in H . Since P is a p -group and Q is a p' -group, we have $P \cap Q = 1$, and thus PQ is the direct product of P and Q .

Now let $U = \mathbf{O}_p(G)$, so that U is a p -group, and observe that PQ acts on U by conjugation since $U \triangleleft G$. We argue that Q fixes every element of U that is fixed by P , or equivalently, that Q centralizes $\mathbf{C}_U(P)$. To see this, observe that $\mathbf{C}_U(P) \subseteq U \cap \mathbf{N}_G(P) = U \cap H$. But $U \cap H$ is a normal p -subgroup of H , and Q is a normal p' -subgroup of H , and so Q centralizes $U \cap H$, and hence it centralizes $\mathbf{C}_U(P)$, as wanted. We conclude by the $P \times Q$ lemma that $Q \subseteq \mathbf{C}_G(U)$. But G is p -solvable and we are assuming that $\mathbf{O}_{p'}(G) = 1$, and thus U contains its own centralizer in G . (This is Lemma 1.2.3 of Hall and Higman, which is our Lemma 3.21.) We now have $Q \subseteq \mathbf{C}_G(U) \subseteq U$, and since Q is a p' -group and U is a p -group, we deduce that $Q = 1$, as required in this case.

In the general situation, let $N = \mathbf{O}_{p'}(G)$ and write $\overline{G} = G/N$, so that $\mathbf{O}_{p'}(\overline{G}) = 1$. If $H \subseteq G$ is p -local, then since $|N|$ is not divisible by p , Lemma 2.17 guarantees that \overline{H} is p -local in \overline{G} , and thus by the first part of the proof, $\mathbf{O}_{p'}(\overline{H}) = 1$. Now \overline{Q} is a normal p' -subgroup of \overline{H} , and so $\overline{Q} \subseteq \mathbf{O}_{p'}(\overline{H}) = 1$. Finally, since $\overline{Q} = 1$, we have $Q \subseteq N$, and the proof is complete. ■

We return now to the situation considered at the beginning of this section. We had A acting coprimely on G via automorphisms, and either G or A is solvable, and we showed in Lemma 4.28 that $G = \mathbf{C}_G(A)[G, A]$. As the following result of H. Fitting shows, more is true if G is abelian.

4.34. Theorem (Fitting). *Let A act via automorphisms on an abelian group G , and assume that A and G are finite and that $(|G|, |A|) = 1$. Then $G = \mathbf{C}_G(A) \times [G, A]$.*

Proof. As G is abelian, both factors are normal, and so it suffices to show that $G = \mathbf{C}_G(A)[G, A]$ and that $\mathbf{C}_G(A) \cap [G, A] = 1$. Of course, G is solvable, and so we can appeal to Lemma 4.28 to deduce the first of these two facts, and so it suffices to prove the second.

Let $\theta : G \rightarrow G$ be the map defined by

$$\theta(g) = \prod_{b \in A} g^b,$$

and note that since G is abelian, the order of the factors in this product is irrelevant, and hence θ is well defined. Also, if $x, y \in G$, then $(xy)^b = x^b y^b$ for all $b \in A$, and so again using the fact that G is abelian, it is easy to see that $\theta(xy) = \theta(x)\theta(y)$, and thus θ is a homomorphism.

If $g \in \mathbf{C}_G(A)$, then $g^b = g$ for all $b \in A$, and thus $\theta(g) = g^{|A|}$. Also, since $|A|$ is coprime to $|G|$, we see that $g^{|A|} \neq 1$ if $g \neq 1$, and thus $\mathbf{C}_G(A) \cap \ker(\theta) = 1$. To complete the proof, therefore, it is enough to show that $[G, A] \subseteq \ker(\theta)$, and since $[G, A]$ is generated by commutators of the form $[g, a]$, with $g \in G$ and $a \in A$, it suffices to prove that each of these commutators lies in $\ker(\theta)$.

If $g \in G$ and $a \in A$, then

$$\theta(g^a) = \prod_{b \in A} g^{ab} = \theta(g),$$

where the second equality holds because ab runs over A as b runs over A . It follows that

$$\theta([g, a]) = \theta(g^{-1}g^a) = \theta(g^{-1})\theta(g^a) = \theta(g)^{-1}\theta(g) = 1.$$

This completes the proof. ■

An easy application of Fitting's theorem is the following.

4.35. Corollary. *Let A act on G via automorphisms, where G is an abelian p -group, and assume that A is a finite p' -group. If A fixes every element of order p in G , then A acts trivially on G .*

Proof. By Fitting's theorem, $G = \mathbf{C}_G(A) \times [G, A]$, and by hypothesis, $\mathbf{C}_G(A)$ contains every element of order p in G . Since $\mathbf{C}_G(A)$ and $[G, A]$ have only the identity in common, it follows that $[G, A]$ contains no elements of order p . But $[G, A]$ is a p -group and every nontrivial p -group contains elements of order p . We conclude that $[G, A] = 1$, and the proof is complete. ■

Surprisingly, the hypothesis that G is abelian in Corollary 4.35 is unnecessary if $p > 2$.

4.36. Theorem. *Let A act on G via automorphisms, where G is a p -group with $p > 2$, and assume that A is a finite p' -group. If A fixes every element of order p in G , then A acts trivially on G .*

The idea of the proof of Theorem 4.36 is quite simple. We show that if G is a minimal counterexample, then there is an abelian counterexample of the same order, and this contradicts Corollary 4.35. It is straightforward to show that a minimal counterexample would have nilpotence class at most 2 (and that does not require that $p > 2$). But getting from class 2 to abelian seems to require a new idea: a remarkable trick due to R. Baer.

4.37. Lemma (Baer trick). *Let G be a finite nilpotent group of odd order and nilpotence class at most 2. Then there exists an addition operation $x + y$ defined for elements $x, y \in G$ such that G is an abelian group with respect to addition. Also, the following hold.*

- (a) *If $xy = yx$ for $x, y \in G$, then $x + y = xy$.*
- (b) *The additive order of each element of G is equal to its multiplicative order.*
- (c) *Every automorphism of G is also an automorphism of the additive group $(G, +)$.*

Before we begin the proof of Baer's lemma, we introduce a bit of suggestive notation. If m is an integer and G is a group of order relatively prime to m , then the map $x \mapsto x^m$ has an inverse, namely the map $x \mapsto x^n$, where n is chosen so that $mn \equiv 1 \pmod{|G|}$. Given $x \in G$, therefore, there is a unique element $y \in G$ such that $y^m = x$, and in fact, y is a power of x . In the case where $|G|$ is odd and $m = 2$, we write $y = \sqrt{x}$ to denote the unique element with square x , and we observe that if $H \subseteq G$ is any subgroup, then $\sqrt{h} \in H$ for every element $h \in H$. Also, it is easy to see that $\sqrt{x^{-1}} = (\sqrt{x})^{-1}$ and that if x and y commute, then $\sqrt{xy} = \sqrt{x}\sqrt{y}$.

Proof of Lemma 4.37. Let $x + y = xy\sqrt{[y, x]}$. To show that $x + y = y + x$ for all $x, y \in G$, we must check that $yx\sqrt{[x, y]} = xy\sqrt{[y, x]}$. This is equivalent to $y^{-1}x^{-1}yx = \sqrt{[y, x]}(\sqrt{[x, y]})^{-1}$. But $(\sqrt{[x, y]})^{-1} = \sqrt{[x, y]^{-1}} = \sqrt{[y, x]}$, and so the identity we must establish is $[y, x] = (\sqrt{[y, x]})^2$, which is clearly true.

Observe that if x and y commute, then $[y, x] = 1$, and since $\sqrt{1} = 1$, it follows that $x + y = xy$, and this establishes (a). In particular, since 1 and x commute, we have $1 + x = 1x = x$ for all $x \in G$, and thus 1 is an additive identity. Also, x and x^{-1} commute, and hence $x + x^{-1} = xx^{-1} = 1$, and thus x^{-1} is the additive inverse of x .

We have

$$x + (y + z) = x + yz\sqrt{[z, y]} = xyz\sqrt{[z, y]}\sqrt{[yz\sqrt{[z, y]}, x]}.$$

Since we are assuming that G has class at most 2, all commutators in G are central, and thus the map $[\cdot, x]$ is a homomorphism. It follows that

$$[yz\sqrt{[z, y]}, x] = [y, x][z, x][\sqrt{[z, y]}, x],$$

and we observe that the third factor is trivial since $[z, y] \in \mathbf{Z}(G)$, and hence $\sqrt{[z, y]} \in \mathbf{Z}(G)$. We now have

$$x + (y + z) = xyz\sqrt{[z, y]}\sqrt{[y, x][z, x]} = xyz\sqrt{[z, y][y, x][z, x]},$$

where the second equality holds because $[z, y]$, commutes with $[y, x][z, x]$. On the other hand,

$$(x + y) + z = xy\sqrt{[y, x]} + z = xy\sqrt{[y, x]}z\sqrt{[z, xy\sqrt{[y, x]}]},$$

and this can be simplified in a similar manner. (Here, we use the fact that $[z, \cdot]$ is a homomorphism.) We obtain

$$(x + y) + z = xyz\sqrt{[y, x][z, x][z, y]},$$

which is equal to the result of our previous computation since the commutators commute. This shows that addition on G is associative, and hence $(G, +)$ is a group.

We have already proved (a). For (b), we use the customary notation for additively written groups, and we write nx to denote the sum of n copies of x , where n is a positive integer and $x \in G$. We argue by induction on n that $nx = x^n$, which is certainly valid for $n = 1$. For $n > 1$, we have

$$nx = x + (n - 1)x = x + x^{n-1} = xx^{n-1} = x^n,$$

where the second equality holds by the inductive hypothesis and the third holds by (a), since x and x^{n-1} commute in G . It follows that $nx = 1$ if and only if $x^n = 1$, and since 1 is the additive identity (as well as the multiplicative identity), it follows that the additive and multiplicative orders of x are equal.

Finally, the addition in G is uniquely determined by the multiplication, and thus any permutation of the elements of G that preserves the multiplication will also preserve the addition. Assertion (c) follows and the proof is complete. ■

Proof of Theorem 4.36. We can assume that $G > 1$, and we proceed by induction on G . If $H < G$ and H admits the action of A , then since every element of order p in H is fixed by A , the inductive hypothesis guarantees that A acts trivially on H , and hence $[H, A] = 1$. In particular, if $[G, A] < G$, then since $[G, A]$ admits A , we have $1 = [G, A, A] = [G, A]$, and there is

nothing further to prove in this case. (The second equality holds, of course, by Lemma 4.29, which applies since $(|G|, |A|) = 1$.)

The derived subgroup G' is characteristic in G , and hence it admits A . Also, the p -group G is certainly solvable, and thus $G' < G$. We deduce that $[G', A] = 1$, and so $[G', A, G] = 1$. Also, since $G' \triangleleft G$, we have $[G, G'] \subseteq G'$, and thus $[G, G', A] \subseteq [G', A] = 1$. The three-subgroups lemma now yields $[A, G, G'] = 1$. But $[A, G] = [G, A] = G$, and so $[G, G'] = 1$ and $G' \subseteq \mathbf{Z}(G)$. In other words, the nilpotence class of G is at most 2, and we can apply the Baer trick to construct the abelian group structure $(G, +)$ on the underlying set of G .

Now an element $a \in A$ induces an automorphism of G , and we conclude by Lemma 4.37(c) that this permutation of the elements of G is also an automorphism of $(G, +)$. In other words, A acts via automorphisms on the abelian group $(G, +)$. By Lemma 4.37(b), the elements of order p in $(G, +)$ are exactly the elements of order p in G , and by hypothesis, they are all fixed by A . By Corollary 4.35, therefore, A acts trivially on $(G, +)$, and hence its action on G is trivial. ■

A similar argument allows us to prove a stronger version of the Thompson $P \times Q$ lemma in the case where p is odd. Recall that in Theorem 4.31 we had a group $A = PQ$ acting on a p -group G , where P is a p -subgroup and Q is a p' -subgroup of A , and both are normal in A . (And we assumed that $\mathbf{C}_G(P) \subseteq \mathbf{C}_G(Q)$.) We now drop the assumption that $P \triangleleft A$.

4.38. Theorem. *Let A be a finite group that acts via automorphisms on a p -group G , where $p > 2$, and let P and Q be subgroups of A . Suppose that P is a p -group and that $Q \triangleleft A$ and Q is a p' -group. Assume also that Q fixes every element of G fixed by P . Then Q acts trivially on G .*

Proof. First, observe that both G and Q are normalized by A in the semidirect product $G \rtimes A$. Therefore $[G, Q]$ is A -invariant, and it admits the action of A .

Now assume that G is abelian, so that by Fitting's theorem, $G = \mathbf{C}_G(Q) \times [G, Q]$. If $[G, Q] > 1$, then by Lemma 4.32 applied to the action of P on $[G, Q]$, we have $\mathbf{C}_{[G, Q]}(P) > 1$. Thus P has nontrivial fixed points in $[G, Q]$, and by hypothesis, these P -fixed points are also Q -fixed points. This is a contradiction, however, since $[G, Q] \cap \mathbf{C}_G(Q) = 1$, and it follows that $[G, Q] = 1$ in this case, as wanted.

Now for the general case, we can assume that $G > 1$. We proceed by induction on G , observing that if $H < G$ and H admits the action of A , then the inductive hypothesis yields that $[H, Q] = 1$. In particular, since $[G, Q]$ admits the action of A , we see that if $[G, Q] < G$, then $1 =$

$[G, Q, Q] = [G, Q]$, and we are done. We can assume, therefore, that $[G, Q] = G$. Now $G' < G$ admits the action of A , and hence $[G', Q] = 1$, and we have $[G', Q, G] = 1$ and $[G, G', Q] \subseteq [G', Q] = 1$. Thus $[Q, G, G'] = 1$, and since $[Q, G] = [G, Q] = G$, we conclude that $G' \subseteq \mathbf{Z}(G)$. Thus G has nilpotence class at most 2, and we can apply the Baer trick.

Now A acts on the abelian group $(G, +)$ and every element fixed by P is fixed by Q . But we have already proved the theorem for abelian groups, and so we deduce that Q acts trivially on $(G, +)$, and hence also on G . ■

Problems 4D

4D.1. Let A act via automorphisms on G , and assume that $N \triangleleft G$ admits A and that $N \supseteq \mathbf{C}_G(N)$. Assume that $(|N|, |A|) = 1$.

- (a) If A acts trivially on N , show that its action on G is trivial.
- (b) If A acts faithfully on G , show that its action on N is faithful.

Hint. For (a) show that $[G, A] \subseteq N$. Consider $\mathbf{C}_\Gamma(N)$, where $\Gamma = G \rtimes A$.

Note. If G is solvable and $N = \mathbf{F}(G)$, then $N \supseteq \mathbf{C}_G(N)$. Also, if G is p -solvable with $\mathbf{O}_{p'}(G) = 1$ and $N = \mathbf{O}_p(G)$, then $N \supseteq \mathbf{C}_G(N)$. Thus in either of these cases, if A acts faithfully and coprimely on G , then A acts faithfully on N .

4D.2. Let G be nilpotent with class at most 2, and assume $|G|$ is odd. Following the proof of Lemma 4.36, construct an additive structure on G , and (as usual for additively written groups) write $x - y$ to denote the sum of x and the additive inverse of y . Show that $xy - yx = [x, y]$.

4D.3. Let A act via automorphisms on G , where $(|G|, |A|) = 1$, and assume that one of A or G is solvable. Suppose that A acts trivially on every A -invariant proper subgroup of G , but that the action of A on G is nontrivial. Prove all of the following.

- (a) G is a p -group.
- (b) $G' \subseteq \mathbf{Z}(G)$.
- (c) No A -invariant subgroup H exists with $G' < H < G$.
- (d) G/G' is elementary abelian.
- (e) G' is elementary abelian (and possibly trivial).
- (f) If $p > 2$, then $x^p = 1$ for all $x \in G$.
- (g) If $p = 2$, then $x^4 = 1$ for all $x \in G$.

Hint. For (c), apply Fitting's theorem to the action of A on G/G' .

4D.4. Let A act via automorphisms on G , where G is a 2-group and A has odd order. Show that if A fixes every element $x \in G$ such that $x^4 = 1$, then the action of A on G is trivial.

4D.5. Let A be solvable with derived length n , and suppose that A acts faithfully via automorphisms on an abelian group B , where $(|B|, |A^{(n-1)}|) = 1$. Show that $G = B \rtimes A$ has derived length $n + 1$. Deduce that there exist solvable groups with arbitrarily large derived lengths.

Hint. For the second part, suppose A has derived length n and let C be cyclic of prime order p not dividing $|A^{(n-1)}|$. Show that if $G = G \wr A$ is the regular wreath product, then G has derived length $n + 1$.

4D.6. Let $\theta : G \rightarrow G$ be the map that appeared in our proof of Fitting's theorem (Theorem 4.34.) Show that (in the notation of that theorem) $\theta(G) = \mathbf{C}_G(A)$ and $\ker(\theta) = [G, A]$.

4D.7. Let G be p -solvable, and suppose that a Sylow p -subgroup of G is cyclic. Let $K \subseteq G$ be a p' -subgroup, and suppose that p divides $|\mathbf{N}_G(K)|$. Show that $K \subseteq \mathbf{O}_{p'}(G)$.

Hint. Induct on $|G|$. If $\mathbf{O}_{p'}(G) > 1$, apply the inductive hypothesis to $\overline{G} = G/\mathbf{O}_{p'}(G)$. Otherwise, show that G has a normal Sylow p -subgroup.

Transfer

5A

We seek results that can be used to prove that a group is not simple. In other words, we want to find techniques that can produce normal subgroups of a group G , or equivalently, homomorphisms θ from G into some group H , and we want to find hypotheses sufficient to guarantee that $\ker(\theta)$ is neither trivial nor is the whole group G . As we shall see, the “transfer” homomorphism, which we discuss in this chapter, is a powerful tool for proving such “good” theorems.

What groups H are available to serve as targets for homomorphisms from G ? One possibility, of course, is to take H to be a symmetric group S_n . (Recall that this was how we proved Theorem 1.1 and its corollaries.) Another useful and well studied situation is where H is the group of invertible $n \times n$ matrices over a field F . (Recall that this group is the general linear group, denoted $GL(n, F)$.) A homomorphism from G into $GL(n, F)$ is called an **F -representation** of G , and representation theory has proven to be a fertile source of good theorems, especially when the field F is taken to be the complex numbers \mathbb{C} . We digress to mention that an F -representation θ of G determines a function $\chi : G \rightarrow F$, called the **character** associated with θ , which is defined by setting $\chi(g)$ to be the trace of the matrix $\theta(g)$. Perhaps surprisingly, it turns out that in the case where $F = \mathbb{C}$, it suffices to study these characters in order to determine most of the interesting properties of the corresponding representations. In particular, it is not terribly difficult to prove that $\ker(\theta) = \{g \in G \mid \chi(g) = \chi(1)\}$, and so characters can be used as proxies for \mathbb{C} -representations in order to prove good theorems. Indeed, it is character theory that provided W. Burnside with the key to his

$p^a q^b$ -theorem, which asserts that a group whose order has exactly two prime divisors cannot be simple.

We can also choose subgroups of G to serve as targets for homomorphisms defined on G . That is approximately what the transfer is: a certain homomorphism from G into an arbitrary subgroup H . As we shall see, however, technical considerations necessitate that the target group for the transfer homomorphism should be abelian, and so instead of a subgroup H , we use its commutator factor group H/H' as the target.

Let G be an arbitrary (not necessarily finite) group, and let $H \subseteq G$ be a subgroup of finite index. In this section, we define the transfer map $v : G \rightarrow H/H'$, and we prove that it is a homomorphism. We start by fixing a set of representatives for the right cosets of H in G . Such a set, called a **right transversal** for H in G , is simply a set of elements of G chosen so that each right coset of H contains exactly one member of the set. If T is a right transversal for H in G , therefore, the right cosets Ht for $t \in T$ are distinct, and they are all of the right cosets of H in G . We can thus use the elements of T as labels for the right cosets of H , and in particular, $|T| = |G : H|$.

Recall that G acts by right multiplication on the set of right cosets of H , and so we can write $(Hx) \cdot g = Hxg$ for each right coset Hx of H in G and each element $g \in G$. Since the elements of the right transversal T can be viewed as labels for the right cosets of H , the action of G on the set $\{Ht \mid t \in T\}$ of right cosets uniquely determines an action of G on T , and we define $t \cdot g$ accordingly. In particular, $(Ht) \cdot g = H(t \cdot g)$, or in other words, if $t \in T$ and $g \in G$, then $t \cdot g$ is the unique element of T that lies in the coset $(Ht) \cdot g = Htg$. Since our "dot" action of G on T is really just the action of G on the right cosets of H , we see, for example, that the stabilizer in G of an element $t \in T$ is exactly the stabilizer of the coset Ht , which we know is H^t . Most importantly, since we know that right multiplication on right cosets really is an action, it follows that the dot action of G on T is a true action, and thus, for example, $(t \cdot x) \cdot y = t \cdot (xy)$ for $t \in T$ and $x, y \in G$.

Now suppose that $t \in T$ and $g \in G$. Then $tg \in Htg = H(t \cdot g)$, and hence there is a unique element $h \in H$ such that $tg = h(t \cdot g)$. Since $tg(t \cdot g)^{-1} = h$, it follows that for all elements $t \in T$ and $g \in G$, we have $tg(t \cdot g)^{-1} \in H$. Given $g \in G$, we would like to multiply all of the elements $tg(t \cdot g)^{-1}$ for $t \in T$ to obtain an element of H depending on g . There is an obvious difficulty here, however, since if H is nonabelian, the order in which this multiplication is carried out may matter. In order to resolve this issue, we suppose that some specific (but arbitrary) ordering of the elements of T has

been declared, and we let $V : G \rightarrow H$ be the function defined by the formula

$$V(g) = \prod_{t \in T} tg(t \cdot g)^{-1},$$

where in computing the product, the elements $t \in T$ are taken in the specified order. Although this nomenclature is not standard, we refer to any map $V : G \rightarrow H$ constructed in this way as a **pretransfer** map. There are usually many different pretransfer maps from G to each subgroup H because, in general, the map depends both on the choice of the right transversal T and on the ordering of T .

Given a pretransfer map $V : G \rightarrow H$, where $H \subseteq G$ is an arbitrary subgroup, we can define a new map $v : G \rightarrow H/H'$ by composing V with the canonical homomorphism $h \rightarrow \bar{h}$ from H to $\bar{H} = H/H'$. In other words

$$v(g) = \overline{V(g)},$$

and we observe that since H/H' is abelian and each factor $tg(t \cdot g)^{-1}$ in the product defining $V(g)$ lies in H , it follows that the map v is independent of the specific ordering on T that we used to define V . As we shall see presently, v is also independent of the choice of the right transversal T , and so for each subgroup $H \subseteq G$, the map v is unambiguously defined. It is the **transfer** map from G to H/H' , which is often inaccurately referred to as the transfer from G to H . (Perhaps we should mention that it is customary to use the letter “ v ” for the transfer because in German, “transfer” is “Verlagerung”).

Before we present any theorems or proofs, we introduce some convenient notation. Given two elements x and y in our subgroup H , we can assert that x and y have the same image in H/H' by writing $H'x = H'y$ or $\bar{x} = \bar{y}$. Unfortunately, if either x or y is some complicated expression such as the product defining $V(g)$ above, the coset notation is somewhat unwieldy, and overbars are even worse. For that reason, we introduce the alternative notation $x \equiv y$ to mean the same thing: that $\bar{x} = \bar{y}$. (It would be more correct to write $x \equiv y \pmod{H'}$, but we will usually suppress explicit mention of the modulus when no confusion is likely to arise.)

5.1. Theorem. *Let G be a group, and suppose that H is a subgroup of finite index. Then the transfer map $v : G \rightarrow H/H'$ is independent of the choice of the right transversal used to define it.*

Proof. Let S and T be two right transversals for H in G , and observe that for each element $t \in T$, there is a unique element $s_t \in S$ that lies in the same right coset of H . We can thus write $s_t = h_t t$ for some uniquely determined element $h_t \in H$, and we have

$$S = \{s_t \mid t \in T\} = \{h_t t \mid t \in T\}.$$

Now let $s \in S$ be arbitrary, and let $g \in G$. Then $s = s_t$ for some element $t \in T$ and $s \cdot g$ is the unique element of S in the coset $Hsg = Htg = H(t \cdot g)$. It follows that $s \cdot g = s_{t \cdot g} = h_{t \cdot g}(t \cdot g)$. We thus have

$$sg(s \cdot g)^{-1} = h_{t \cdot g}(h_{t \cdot g}(t \cdot g))^{-1} = h_t(tg(t \cdot g)^{-1})h_{t \cdot g}^{-1}.$$

Writing V_S and V_T to denote pretransfers constructed from S and T , we have

$$\begin{aligned} V_S(g) &= \prod_{s \in S} sg(s \cdot g)^{-1} \equiv \prod_{t \in T} h_t(tg(t \cdot g)^{-1})h_{t \cdot g}^{-1} \\ &\equiv \prod_{t \in T} h_t \prod_{t \in T} tg(t \cdot g)^{-1} \left(\prod_{t \in T} h_{t \cdot g} \right)^{-1}. \end{aligned}$$

Here, the first congruence is not necessarily an equality because we made no assumption about how the arbitrary orderings on S and T are related. The second congruence is valid because we are working modulo H' , and so we are free to rearrange factors that lie in H . Finally, $t \cdot g$ runs over all of T as t does, and thus the first and third factors on the right cancel (modulo H'), and we conclude that $V_S(g) \equiv V_T(g)$, as required. ■

Although it may be reassuring to know that the transfer map from G to H is unambiguously defined, as we have just shown, the really vital fact about the transfer is that it is a homomorphism, and the proof of that fact does not rely on Theorem 5.1.

5.2. Theorem. *Let G be a group, and suppose that H is a subgroup of finite index. Then the transfer map $v : G \rightarrow H/H'$ is a homomorphism.*

Proof. Let T be a right transversal for H in G , and let V be a pretransfer associated with T . For $t \in T$, we have $t \cdot (xy) = (t \cdot x) \cdot y$, and thus

$$t(xy)(t \cdot (xy))^{-1} = (tx(t \cdot x)^{-1})((t \cdot x)y((t \cdot x) \cdot y)^{-1}).$$

Since both factors on the right lie in H , we have

$$\begin{aligned} V(xy) &= \prod_{t \in T} t(xy)(t \cdot (xy))^{-1} \equiv \prod_{t \in T} tx(t \cdot x)^{-1} \prod_{t \in T} (t \cdot x)y((t \cdot x) \cdot y)^{-1} \\ &\equiv V(x)V(y), \end{aligned}$$

where the last congruence holds because $t \cdot x$ runs over all of T as t does. It follows that $v(xy) = v(x)v(y)$, and the proof is complete. ■

Although Theorem 5.2 is not very deep, it enables us to prove the following, which is our first application of transfer theory.

5.3. Theorem. *Suppose that G is a finite group, and let p be a prime divisor of $|G' \cap \mathbf{Z}(G)|$. Then a Sylow p -subgroup of G is nonabelian.*

Proof. Let $P \in \text{Syl}_p(G)$, and assume that P is abelian. Let T be a right transversal for P in G , and consider the transfer homomorphism $v : G \rightarrow P$. Since P is abelian, we have $v = V$, where V is the pretransfer computed using T .

Now $G' \cap \mathbf{Z}(G)$ is a normal subgroup of G with order divisible by p , and so its intersection with the Sylow subgroup P is nontrivial. We can thus choose a nonidentity element $z \in P \cap G' \cap \mathbf{Z}(G)$, and we compute $v(z)$. If $t \in T$, then since $z \in \mathbf{Z}(G)$, we have $Ptz = Pzt = Pt$, where the last equality holds because $z \in P$. Thus t is the element of T in the coset Ptz , and we conclude that $t \cdot z = t$. Then $tz(t \cdot z)^{-1} = tzt^{-1} = z$, where the last equality follows because z is central. We conclude that $v(z) = V(z) = z^{|T|} = z^{|G:P|}$.

On the other hand, v is a homomorphism from G into the abelian group P , and hence the derived subgroup G' is contained in $\ker(v)$. Since $z \in G'$, we have $1 = v(z) = z^{|G:P|}$, and thus z has order dividing the p' -number $|G : P|$. But $z \in P$, and so z has p -power order, and we conclude that $z = 1$. This contradiction shows that P must be nonabelian. ■

5.4. Corollary. *Let $Z \subseteq \mathbf{Z}(\Gamma) \cap \Gamma'$, where Γ is a finite group. Then a Sylow p -subgroup of Γ/Z is noncyclic for every prime divisor p of $|Z|$.*

Proof. Let $P \in \text{Syl}_p(\Gamma)$. We are assuming that p divides $|Z|$ and that $Z \subseteq \mathbf{Z}(\Gamma) \cap \Gamma'$, so it follows by Theorem 5.3 that P is not abelian. Since $P \cap Z \subseteq \mathbf{Z}(P)$ and P is nonabelian, we conclude that $P/(P \cap Z)$ cannot be cyclic. But $P/(P \cap Z) \cong PZ/Z \in \text{Syl}_p(\Gamma/Z)$, and thus Γ/Z has a noncyclic Sylow p -subgroup. ■

We digress to provide some context for Corollary 5.4. Given a finite group G , consider pairs of groups (Γ, Z) , where $Z \subseteq \mathbf{Z}(\Gamma)$ and $\Gamma/Z \cong G$. (We say that Γ is a **central extension** of G in this situation.) Of course, it is trivial to find central extensions of G since we could simply take $\Gamma = G \times Z$, where Z is any abelian group. To prevent this, and to make the situation more interesting, we insist that Z should be contained in the derived subgroup Γ' as well as in the center $\mathbf{Z}(\Gamma)$. With this additional requirement, the problem is much more restrictive. Indeed, one can prove that among all pairs (Γ, Z) , where $Z \subseteq \mathbf{Z}(\Gamma) \cap \Gamma'$ and $\Gamma/Z \cong G$, there is a unique (up to isomorphism) largest group Z that can occur as a second component, and that every other possible second component is a homomorphic image of this largest one. The largest possible second component of a pair (Γ, Z) associated with a given group G is called the **Schur multiplier** of G , and it is denoted $M(G)$.

If (Γ, Z) is one of our pairs in which $Z \cong M(G)$, then, of course, $|\Gamma| = |G||M(G)|$, and in this case, Γ is said to be a **Schur representation group** for G . If the group G is **perfect**, which, we recall, means that $G' = G$,

then it has a unique (up to isomorphism) Schur representation group, but in general, a given group G can have more than one isomorphism type of Schur representation group. For example, if G is noncyclic of order 4, it is not very hard to show that $|M(G)| = 2$, and thus both the dihedral group D_8 and the quaternion group Q_8 are Schur representation groups for G .

Corollary 5.4 can be restated this way: If p is a prime divisor of $|M(G)|$, then a Sylow p -subgroup of G must be noncyclic, and in particular, it is nontrivial. For example, the only prime p for which a Sylow p -subgroup of the alternating group A_5 is noncyclic is $p = 2$, and it follows that $M(A_5)$ is a 2-group. In fact, the Schur multiplier of A_5 has order 2. (We cannot resist mentioning that $|M(A_n)| = 2$ for all integers $n \geq 4$ except $n = 6$ and $n = 7$; in those two cases, the Schur multiplier has order 6. This is another example of what seems to be common phenomenon in finite group theory: general patterns with finite lists of exceptions.)

Problems 5A

5A.1. Suppose that G is abelian and $H \subseteq G$ has index n . Show that the transfer homomorphism from G to H is the map $g \mapsto g^n$.

5A.2. Show that the transfer homomorphism $v : G \rightarrow G/G'$ is just the canonical homomorphism from G to G/G' .

5A.3. Let $H \subseteq K \subseteq G$, where $|G : H| < \infty$, and suppose that S is a right transversal for H in K and that T is a right transversal for K in G . Write $ST = \{st \mid s \in S, t \in T\}$.

- Show that each element of ST is uniquely of the form st with $s \in S$ and $t \in T$.
- Show that ST is a right transversal for H in G . Deduce that $|G : H| = |G : K||K : H|$.
- Let $s \in S$ and $t \in T$, and suppose that $g \in G$. Show that

$$(st) \cdot g = s \cdot (tg(t \cdot g)^{-1})(t \cdot g).$$

- Let $V_T : G \rightarrow K$ be a pretransfer computed with respect to T , and let $v : K \rightarrow H/H'$ be the transfer homomorphism. Show that the composite map $w : G \rightarrow H/H'$ defined by $w(g) = v(V_T(g))$ is the transfer homomorphism.

5A.4. Let $H \subseteq \mathbf{Z}(G)$, and assume that $|G : H| = n < \infty$. Let $v : G \rightarrow H$ be the transfer homomorphism.

- If $h \in H$, show that $v(h) = h^n$.

- (b) Now assume that H is finite and that $|H|$ is coprime to n . Show that $G = H \times \ker(v)$.

Note. The fact that H is a direct factor of G in (b) can also be proved by an appeal to the Schur-Zassenhaus theorem.

5A.5. Let G be finite, and suppose C is a cyclic normal subgroup such that G/C is cyclic. Show that $|M(G)|$ divides $|C : G'|$.

Hint. Apply Lemma 4.6 to a group Γ containing a subgroup Z such that $\Gamma/Z \cong G$ and $Z \subseteq \Gamma' \cap \mathbf{Z}(\Gamma)$.

5A.6. Let D be dihedral of order 2^n where $n \geq 2$. Show that the Schur multiplier $M(D)$ has order 2.

5A.7. Let B and C be cyclic subgroups of a finite group G , and suppose that $BC = G$ and $B \cap C > 1$. As in Problem 5A.5, assume that $C \triangleleft G$ and that $|C : G'| = n$. Show that the order of $M(G)$ is strictly less than n .

Note. In particular, semidihedral and generalized quaternion groups have trivial Schur multipliers.

5A.8. Let A and B be arbitrary finite groups.

- (a) Show that $|M(A \times B)| \geq |M(A)||M(B)|$.
 (b) Assuming that $|A|$ and $|B|$ are coprime, show that $M(A \times B) \cong M(A) \times M(B)$.

5B

It is often difficult to obtain useful information about the transfer map if we work directly from the definition. But if we appeal to the transfer-evaluation lemma, which we present in this section, computations become easier, and transfer becomes more useful as a tool for proving theorems.

We continue to allow our groups to be infinite, but of course, in order for the transfer from a group G to a subgroup H to be defined, we must assume that the index $|G : H|$ is finite.

5.5. Lemma (Transfer Evaluation). *Let G be a group, and let H be a subgroup with finite index n . Let $V : G \rightarrow H$ be a pretransfer map constructed using a right transversal T for H in G , and fix an element $g \in G$. Then there exist a subset $T_0 \subseteq T$ and positive integers n_t for $t \in T_0$ (depending on g) such that the following hold.*

- (a) $tg^{n_t}t^{-1} \in H$ for all $t \in T_0$.
 (b) $V(g) \equiv \prod_{t \in T_0} tg^{n_t}t^{-1}$.

$$(c) \sum_{t \in T_0} n_t = n.$$

(d) If g has finite order m , then n_t is a divisor of m for all $t \in T_0$.

Of course, the product in assertion (b) is not well defined unless some order in which to take the factors is established. This is really irrelevant, however, since we are working modulo H' and by (a), each factor $tg^{n_t}t^{-1}$ lies in H . If H happens to be abelian, so that $H' = 1$, then of course, assertion (b) says that $v(g) = \prod tg^{n_t}t^{-1}$, where v is the transfer map.

Proof of Lemma 5.5. The cyclic subgroup $\langle g \rangle \subseteq G$ acts on T via our “dot” action, and thus T decomposes into $\langle g \rangle$ -orbits. Let $T_0 \subseteq T$ be a set of representatives of these orbits (so that each orbit contains exactly one member of T_0) and let n_t be the size of the orbit containing $t \in T_0$. Of course, the sum of the orbit sizes is $|T| = n$, and this establishes (c). Also, (d) is immediate since if $o(g) = m < \infty$, then $|\langle g \rangle| = m$, and so the size of each $\langle g \rangle$ -orbit on T divides m .

Now let \mathcal{O} be a $\langle g \rangle$ -orbit on T , and let $t \in T_0$ lie in \mathcal{O} , so that $|\mathcal{O}| = n_t$. Since

$$\mathcal{O} = \{t \cdot x \mid x \in \langle g \rangle\} = \{t \cdot g^i \mid i \in \mathbb{Z}\},$$

we observe that the elements $t \cdot g^i$ must be distinct for $0 \leq i < n_t$, and that these are exactly the elements of \mathcal{O} . Also, it should be clear that $t \cdot g^{n_t} = t$.

Recall that for every element $s \in T$, we have $sg(s \cdot g)^{-1} \in H$, and the product of these elements (in some order) is equal to $V(g)$. Taking $s = t \cdot g^i$, we have

$$(t \cdot g^i)g(t \cdot g^{i+1})^{-1} = sg(s \cdot g)^{-1} \in H$$

for all integers i . Since $t \cdot g^{n_t} = t$, we see that the product of the elements of this form with $0 \leq i \leq n_t - 1$ (taken in order of increasing i) is precisely $tg^{n_t}t^{-1}$, which therefore lies in H . This proves (a), and it shows that except possibly for the order of the factors, the element $tg^{n_t}t^{-1}$ is the contribution to the product defining $V(g)$ coming from the elements of T that lie in \mathcal{O} . Since T is the union of the various orbits and T_0 is a set of representatives of these orbits, assertion (b) follows. ■

As our first application of the transfer-evaluation lemma, we compute the transfer into a central subgroup.

5.6. Theorem. *Let G be a group, and suppose that Z is a central subgroup of finite index n . Then the transfer from G to Z is the map $g \mapsto g^n$. This map is therefore a homomorphism from G into Z .*

Note that since Z is abelian, the transfer to Z really does map to Z ; there is no need to work modulo anything. Also, observe that Theorem 5.6

generalizes both Problem 5A.1 and Problem 5A.4(a). Finally, we mention that since, in the situation of the theorem, G/Z is a group of order n , it is obvious that $g^n \in Z$. What is not at all obvious, however, is that the map $g \mapsto g^n$ is a homomorphism, so that $(xy)^n = x^n y^n$ for all $x, y \in G$.

Proof of Theorem 5.6. Choose a right transversal T for Z in G and let $g \in G$. Choose a subset $T_0 \subseteq T$ and integers n_t for $t \in T_0$, as in the transfer-evaluation lemma (5.5). For $t \in T_0$, therefore, we have $tg^{n_t}t^{-1} \in Z$, and since $Z \subseteq \mathbf{Z}(G)$, we have

$$tg^{n_t}t^{-1} = (tg^{n_t}t^{-1})^t = t^{-1}(tg^{n_t}t^{-1})t = g^{n_t}.$$

By Lemma 5.5(b), the product over $t \in T_0$ of these elements is $v(g)$, where $v : G \rightarrow Z$ is the transfer. Since $\sum n_t = n$, however, this product is g^n . ■

We digress from our study of the transfer to discuss an application of Theorem 5.6.

5.7. Theorem (Schur). *Suppose that $\mathbf{Z}(G)$ has finite index in a group G . Then G' is a finite subgroup.*

We need a few preliminary results. First, we show that in the situation of Schur's theorem, there are only finitely many commutators in G . Of course, this falls far short of the assertion of the theorem since in general, not every element of G' is a commutator.

5.8. Lemma. *Let T be a right transversal for $\mathbf{Z}(G)$ in a group G . Then every commutator in G has the form $[s, t]$, where $s, t \in T$. In particular, if $|G : \mathbf{Z}(G)| < \infty$, then there are only finitely many different commutators.*

Proof. The second statement follows from the first since $|T| = |G : \mathbf{Z}(G)|$. To prove the first assertion, observe that every element of G can be written in the form xs , where $x \in \mathbf{Z}(G)$ and $s \in T$. To complete the proof, therefore, it suffices to show that $[xs, yt] = [s, t]$, where $x, y \in \mathbf{Z}(G)$ and $s, t \in T$. We have $[xs, yt] = [x, yt]^s [s, yt] = [s, yt]$, where the second equality holds because $[x, yt] = 1$ since x is central. Also, $[s, yt] = [yt, s]^{-1} = ([y, s]^t [t, s])^{-1} = [t, s]^{-1} = [s, t]$, where the third equality holds since y is central. ■

We also need the following easy consequence of Theorem 5.6.

5.9. Corollary. *Suppose that G is a group and that $|G : \mathbf{Z}(G)| = n$. Then the n th power of every commutator in G is the identity.*

Proof. The map $g \mapsto g^n$ is a homomorphism from G into the abelian group $\mathbf{Z}(G)$, and thus the commutator subgroup G' is contained in its kernel. ■

The final ingredient in the proof of Theorem 5.7 is the following somewhat more general fact due to A. P. Dietzmann.

5.10. Theorem (Dietzmann). *Let G be a group, and let $X \subseteq G$ be a finite subset that is closed under conjugation. Assume that there is a positive integer n such that $x^n = 1$ for all $x \in X$. Then $\langle X \rangle$ is a finite subgroup of G .*

Proof. Let S be the subset of G consisting of all products of finitely many members of X , allowing repeats, and allowing the “empty” product, which is equal to 1. Then S is closed under multiplication, and also, since $x^n = 1$ for each element $x \in X$, we see that $x^{-1} = x^{n-1}$ lies in S . It follows that S is closed under inverses, and hence $S = \langle X \rangle$. Every element of $\langle X \rangle$, therefore, is a product of members of X , and we will show that it is never necessary to use more than $(n-1)|X|$ factors. Since X is finite, it will follow that $\langle X \rangle$ is finite, as wanted.

Consider an arbitrary product $g = x_1 x_2 \cdots x_m$ of m not necessarily distinct elements of X , and suppose that some particular element $x \in X$ occurs at least k times among the factors x_i , where $k \geq 1$. We argue that g can be rewritten as a product of m elements of X in such a way that the first factor is x , and there are still a total of at least k factors equal to x . To see why this is true, suppose that t is the smallest subscript such that $x_t = x$. We can assume that $t > 1$, and we observe that

$$\begin{aligned} x_1 x_2 \cdots x_{t-1} x_t &= x_1 x_2 \cdots x_{t-1} x = x(x_1 x_2 \cdots x_{t-1})^x \\ &= x(x_1)^x (x_2)^x \cdots (x_{t-1})^x. \end{aligned}$$

The expression on the right is a product of t elements of X because X is closed under conjugation by x , and of course, its first factor is x . Also, there are at least $k-1$ copies of x among the elements x_i with $t < i \leq m$, and so if we multiply the above expression on the right by $x_{t+1} \cdots x_m$, we get a new representation of g as a product of m elements of X , and these include a total of at least k copies of x . The first factor in this product is x , as desired.

Assuming now (as we may) that $x_1 = x$, suppose that $k \geq 2$. We can repeat the above argument for the product $x_2 x_3 \cdots x_m$, and so we can assume that $x_2 = x$. Continuing like this, we see that we can assume that g is a product of m elements of X such that the first k factors are all equal to x .

Now fix an arbitrary element $g \in \langle X \rangle$ and write $g = x_1 x_2 x_3 \cdots x_m$, where the factors $x_i \in X$ are not necessarily distinct, and where m is as small as possible. Supposing that $m > (n-1)|X|$, we derive a contradiction. By the “pigeon-hole” principle, at least one element $x \in X$ must occur at least n times among the factors x_i for $1 \leq i \leq m$, and by the above reasoning, it is no loss to assume that the first n factors are all copies of x . But $x^n = 1$,

and thus $g = x_{n+1}x_{n+2} \cdots x_m$ is a product of $m - n$ elements of X . This is the desired contradiction by the assumed minimality of m . ■

Finally, we assemble the pieces to obtain a proof of Schur's theorem.

Proof of Theorem 5.7. Let X be the set of all commutators in G , and observe that $|X|$ is finite by Lemma 5.8. Also, since $[x, y]^g = [x^g, y^g]$ for x, y and g in G , we see that X is closed under conjugation. Now write $n = |G : \mathbf{Z}(G)|$, so that by Corollary 5.9, we have $x^n = 1$ for all $x \in X$. The result now follows by Theorem 5.10. ■

Problems 5B

5B.1. Let G be finite, and suppose that $P \in \text{Syl}_p(G)$ and that $g \in P$ has order p . If $g \in G'$, but $g \notin P'$, show that $g^t \in P'$ for some element $t \in G$ with $t \notin P$.

Hint. Let v be the transfer homomorphism from G to P/P' and observe that $g \in \ker(v)$, and thus $V(g) \in P'$, where V is a corresponding pretransfer map. Apply the transfer-evaluation lemma, and note that each integer n_t is either 1 or p .

5B.2. In the situation of Theorem 5.10, suppose $|X| = m$. Show that $|\langle X \rangle| \leq n^m$.

Hint. Write $X = \{x_1, x_2, \dots, x_m\}$ and show that every element of $\langle X \rangle$ has the form $(x_1)^{e_1}(x_2)^{e_2} \cdots (x_m)^{e_m}$, where the e_i are integers satisfying $0 \leq e_i < n$.

5B.3. Let G be an arbitrary group. Show that an element $x \in G$ lies in some finite normal subgroup of G if and only if x has finite order and its conjugacy class in G has finite size.

5C

We return now to finite groups. If we want to use transfer theory to prove that some group G is not simple, we need to choose a subgroup $H \subseteq G$, and we must show that the kernel of the transfer homomorphism $v : G \rightarrow H/H'$ is neither trivial nor the whole group G . If H is proper in G , then automatically, $\ker(v) > 1$ since in that case, v cannot be injective. (Recall that we are assuming that G is finite.) To prove “good” nonsimplicity theorems, therefore, it is sufficient to find conditions that will guarantee that $\ker(v) < G$, or equivalently that there exists at least one element $x \in G$ such that $v(x) \neq 1$.

Given an element $x \in G$, it is sometimes easier to compute $v(x)$ if x happens to lie in the transfer target H . Of course, if we limit our attention to elements of H and we can show that not every element of H lies in $\ker(v)$, this is good enough. (Obviously, if $H \not\subseteq \ker(v)$, then $\ker(v) < G$, and in that case, G is not simple.) In fact, if H is a Sylow subgroup of G , or more generally, if H is a Hall subgroup, then the converse of this assertion is true too: if $\ker(v) < G$, then $H \not\subseteq \ker(v)$. In the situation where H is a Hall subgroup, therefore, we lose nothing by computing the transfer only on elements of H . The following easy lemma proves somewhat more than this.

5.11. Lemma. *Let H be a Hall subgroup of a finite group G , and let $v : G \rightarrow H/H'$ be the transfer homomorphism. Then $v(H) = v(G)$, and so $|H : H \cap \ker(v)| = |G : \ker(v)|$.*

Proof. We know that $|G : \ker(v)| = |v(G)|$, and since $v(G) \subseteq H/H'$, we deduce that $|G : \ker(v)|$ divides $|H|$. Then $|G : \ker(v)|$ is coprime to $|G : H|$, and so $\ker(v)H = G$ by Lemma 3.16. The result now follows. ■

Again let $H \subseteq G$, and consider the transfer homomorphism $v : G \rightarrow H/H'$. When we apply the transfer-evaluation lemma to compute $v(x)$ for some element $x \in G$, we are led to consider elements of H of the form $tx^{n_t}t^{-1}$ for certain elements $t \in G$ and positive exponents n_t . If $x \in H$, which as we now know is often the case of interest, then also $x^{n_t} \in H$. In this situation, the elements x^{n_t} and $tx^{n_t}t^{-1}$ both lie in H , and they are clearly conjugate in G (via the element t), but of course, they need not be conjugate in H .

Motivated by this, we consider the intersection of a conjugacy class X of G with a subgroup H , where we assume that $X \cap H$ is nonempty. Clearly, if $x \in X \cap H$ and y lies in the conjugacy class of H containing x , then $y \in X \cap H$, and this shows that $X \cap H$ is a union of conjugacy classes of H . We say that classes Y_1 and Y_2 of H are **fused** in G if Y_1 and Y_2 are contained in the same class of G . Also, if $H \subseteq K \subseteq G$, we say that K **controls G -fusion** in H if every two classes of H that are fused in G are already fused in K . Equivalently, K controls G -fusion in H if and only if every pair of G -conjugate elements of H are K -conjugate. In particular, G always controls G -fusion in H , and H controls G -fusion in itself precisely when no two distinct classes of H are fused in G . As we shall see, the notion of “control of fusion” is vital for understanding transfer, especially transfer to Sylow subgroups, and more generally, to Hall subgroups.

We begin our study of fusion with the following general result.

5.12. Lemma. *Let $P \in \text{Syl}_p(G)$, where G is a finite group. Then $\mathbf{N}_G(P)$ controls G -fusion in $\mathbf{C}_G(P)$.*

Proof. Assuming that $x, y \in \mathbf{C}_G(P)$ are conjugate in G , we must show that in fact, these elements are conjugate in $\mathbf{N}_G(P)$. Write $y = x^g$ with $g \in G$, and observe that since $x \in \mathbf{C}_G(P)$, we have $y = x^g \in \mathbf{C}_G(P)^g = \mathbf{C}_G(P^g)$. Then $P^g \subseteq \mathbf{C}_G(y)$, and hence P^g is a Sylow p -subgroup of $\mathbf{C}_G(y)$. Also $y \in \mathbf{C}_G(P)$, and so $P \subseteq \mathbf{C}_G(y)$, and hence P is also a Sylow p -subgroup of $\mathbf{C}_G(y)$. We can now apply the Sylow C-theorem in the group $\mathbf{C}_G(y)$ to the two Sylow p -subgroups P and P^g , and we deduce that $(P^g)^c = P$, for some element $c \in \mathbf{C}_G(y)$. Then $gc \in \mathbf{N}_G(P)$ and $x^{gc} = y^c = y$, and so x and y are conjugate in $\mathbf{N}_G(P)$, as required. ■

We can now prove Burnside's normal p -complement theorem. (Recall that if p is a prime, then a normal p -complement in a finite group G is a normal subgroup with index equal to the order of a Sylow p -subgroup. Equivalently, it is a subgroup $N \triangleleft G$ such that $|N|$ is not divisible by p and $|G : N|$ is a power of p . In still other words, a normal p -complement is a normal Hall p' -subgroup. A group that has a normal p -complement is said to be p -**nilpotent**.)

5.13. Theorem (Burnside). *Let $P \in \text{Syl}_p(G)$, where G is a finite group, and suppose $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$. Then G has a normal p -complement.*

Proof. In this situation, P is abelian, so $P \subseteq \mathbf{C}_G(P)$. By Lemma 5.12, therefore, every two elements of P that are conjugate in G are conjugate in $\mathbf{N}_G(P)$. But P is central in $\mathbf{N}_G(P)$, so no two distinct elements of P can be conjugate in $\mathbf{N}_G(P)$. It follows that no two distinct elements of P can be conjugate in G .

Now consider the transfer homomorphism $v : G \rightarrow P$, and recall that in this case, where P is abelian, there is no distinction between the transfer and pretransfer. Let $x \in P$, and apply the transfer-evaluation lemma to compute that

$$v(x) = \prod_{t \in T_0} tx^{n_t}t^{-1},$$

where T_0 is some subset of a right transversal T_i for P in G . Also, $\sum n_t = |G : P|$, and we know that each of the factors $tx^{n_t}t^{-1}$ lies in P . Since $tx^{n_t}t^{-1}$ and x^{n_t} are G -conjugate elements of P , the first paragraph of the proof guarantees that they are equal, and thus $x^{n_t} = tx^{n_t}t^{-1}$ for all $t \in T_0$. Then

$$v(x) = \prod_{t \in T_0} x^{n_t} = x^{|G:P|},$$

and so if $v(x) = 1$, then x has order dividing $|G : P|$. But $x \in P$, and so the order of x also divides $|P|$. It follows that $x = 1$, and hence $P \cap \ker(v) = 1$. By Lemma 5.11, we have $|G : \ker(v)| = |P|$, and so $\ker(v)$ is the desired normal p -complement in G . ■

5.14. Corollary. *Let $P \in \text{Syl}_p(G)$, where G is a finite group and p is the smallest prime divisor of $|G|$, and assume that P is cyclic. Then G has a normal p -complement.*

Proof. We know that $\mathbf{N}_G(P)/\mathbf{C}_G(P)$ can be isomorphically embedded in $\text{Aut}(P)$, which, because P is cyclic, has order $\varphi(|P|)$, where φ is Euler's function. We can certainly assume that $P > 1$, and so we can write $|P| = p^n$, with $n > 0$. Then $\varphi(|P|) = p^{n-1}(p-1)$, and since this number has no prime divisor larger than p , it follows that $|\mathbf{N}_G(P) : \mathbf{C}_G(P)|$ has no prime divisor larger than p . This index also has no prime divisor smaller than p because no such prime divides $|G|$. Finally, the prime p itself does not divide $|\mathbf{N}_G(P) : \mathbf{C}_G(P)|$ since P is abelian, and thus the full Sylow p -subgroup P is contained in $\mathbf{C}_G(P)$. We conclude that $|\mathbf{N}_G(P) : \mathbf{C}_G(P)|$ has no prime divisors at all, and so this index is 1, and $\mathbf{N}_G(P) = \mathbf{C}_G(P)$. In other words, $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$, and hence by Burnside's theorem, G has a normal p -complement. ■

We mention that if some group G has a cyclic Sylow p -subgroup, then the same is true for every subgroup of G and every homomorphic image of G . (For subgroups, this follows by the Sylow D-theorem since a Sylow p -subgroup of a subgroup of G is contained in a Sylow p -subgroup of G . For factor groups, our assertion is a consequence of Problem IB.5, which implies that a surjective homomorphism carries Sylow p -subgroups to Sylow p -subgroups.) In particular, this shows that the hypotheses of the following corollary are inherited by subgroups and factor groups.

5.15. Corollary. *Let G be a finite group, and suppose that all Sylow subgroups of G are cyclic. Then G is solvable.*

Proof. We can assume that $G > 1$, and we proceed by induction on $|G|$. If p is the smallest prime divisor of $|G|$, then G has a normal p -complement N by Corollary 5.14. Also, $N < G$ and all Sylow subgroups of N are cyclic, and thus N is solvable by the inductive hypothesis. Since G/N is a p -group, it is solvable too, and thus G is solvable by Lemma 3.10(e). ■

In particular, it follows that the order of a nonabelian simple group cannot be a product of distinct prime numbers.

Actually, much more can be said about groups in which all Sylow subgroups are cyclic. Not only is such a group solvable, but it is also **metacyclic**, which means that it has a cyclic normal subgroup with a cyclic factor group. The following shows that even more is true.

5.16. Theorem. *Suppose that all Sylow subgroups of the finite group G are cyclic. Then both G' and G/G' are cyclic, and they have coprime orders.*

The key step here is the following.

5.17. Theorem. *Let P be a cyclic Sylow p -subgroup of some finite group G . Then p divides at most one of the numbers $|G'|$ and $|G : G'|$.*

Proof. Let $N = \mathbf{N}_G(P)$, and let $K \subseteq N$ be a complement for P in N . (The existence of K is guaranteed by the Schur-Zassenhaus theorem.) By Fitting's theorem (4.34), we have $P = [P, K] \times \mathbf{C}_P(K)$. If $[P, K] = 1$, then $\mathbf{C}_P(K) = P$, and in this case, P is central in $N = PK$. By Burnside's theorem, therefore, G has a normal p -complement M , and since G/M is a p -group, it must be cyclic. Then $G' \subseteq M$, and so p does not divide $|G'|$.

If, on the other hand, $[P, K] > 1$, then $[P, K]$ contains the unique subgroup of order p in the cyclic group P . It follows that $\mathbf{C}_P(K)$ contains no subgroup of order p , and hence $\mathbf{C}_P(K) = 1$. Therefore $P = [P, K] \subseteq G'$, and so $|G : G'|$ is not divisible by p , as required. ■

We need one further observation: an abelian group in which all Sylow subgroups are cyclic must itself be cyclic. In fact, if we choose a generator x_p of the Sylow p -subgroup of G for each prime divisor p of $|G|$, it is easy to see that the element $\prod x_p$ is a generator for G .

Proof of Theorem 5.16. That no prime can divide both $|G'|$ and $|G : G'|$ follows by Theorem 5.17. Also, G/G' is an abelian group with all Sylow subgroups cyclic, and hence it must be cyclic. To show that G' is cyclic, we proceed by induction on $|G|$. We can assume, of course, that $G > 1$, and thus $G' < G$ because G is solvable by Corollary 5.15. The inductive hypothesis applied to G' tells us that G'' is cyclic, and thus $\text{Aut}(G'')$ is abelian. But $G/\mathbf{C}_G(G'')$ is isomorphically embedded in $\text{Aut}(G'')$, and thus $G/\mathbf{C}_G(G'')$ is abelian, and we have $G' \subseteq \mathbf{C}_G(G'')$. Now G'/G'' is abelian and hence is cyclic, and since $G'' \subseteq \mathbf{Z}(G')$, it follows that G' is abelian, and hence G' is cyclic, as required. ■

Next, we consider what happens if only part of an abelian Sylow p -subgroup P of G is central in $\mathbf{N}_G(P)$. (In the case of Burnside's theorem, where the whole of P is central in $\mathbf{N}_G(P)$, it is automatic that P is abelian, but in this more general situation we must *assume* that P is abelian.) Since Burnside's theorem (5.13) is an easy consequence of the following, we could have omitted the proof of that earlier result, which is hereby rendered redundant. We mention also that the following can also be viewed as a stronger form of Theorem 5.3.

5.18. Theorem. *Let P be an abelian Sylow p -subgroup of a finite group G . Then*

$$G' \cap P \cap \mathbf{Z}(\mathbf{N}_G(P)) = 1.$$

Proof. Let $v : G \rightarrow P$ be the transfer, and let $x \in G' \cap P \cap \mathbf{Z}(\mathbf{N}_G(P))$. Then

$$1 = v(x) = \prod_{t \in T_0} tx^{n_t}t^{-1},$$

where the first equality holds since $x \in G' \subseteq \ker(v)$, and the second follows by the transfer-evaluation lemma, where T_0 and the integers n_t are as usual, and where each factor $tx^{n_t}t^{-1}$ lies in P . Since $x \in P$, both x^{n_t} and $tx^{n_t}t^{-1}$ lie in P , and hence these G -conjugate elements of $P \subseteq \mathbf{C}_G(P)$ are conjugate in $\mathbf{N}_G(P)$ by Lemma 5.12. But x is central in $\mathbf{N}_G(P)$, and thus x^{n_t} is also central in this group, and hence is conjugate only to itself in $\mathbf{N}_G(P)$. It follows that $x^{n_t} = tx^{n_t}t^{-1}$ for all $t \in T_0$, and thus $v(x) = x^{|G:P|}$ because $\sum n_t = |G : P|$. Thus $1 = x^{|G:P|}$, and x has p' -order. Since $x \in P$, we conclude that $x = 1$, as desired. ■

As an application of Theorem 5.18, we offer the following.

5.19. Corollary. *Suppose that a Sylow 2-subgroup of a nonabelian finite group G is a direct product of cyclic subgroups, one of which is strictly larger than all of the others. Then G is not simple.*

Proof. Let $P \in \text{Syl}_2(G)$. We can write $P = A \times B$, where A is cyclic of order $a \geq 2$, and where $x^{a/2} = 1$ for all $x \in B$. Let $C = \{x^{a/2} \mid x \in P\}$, and observe that C is a nontrivial characteristic subgroup of P of order 2, and thus the unique nonidentity element t of C is central in $\mathbf{N}_G(P)$. It follows by Theorem 5.18 that $t \notin G'$, and thus $G' < G$. If G is simple, then $G' = 1$, and so G is abelian, and this is a contradiction. ■

We mention that it is known from a part of the simple group classification that if a Sylow 2-subgroup of a simple group is abelian, then in fact, it must be elementary abelian. In other words, all of its cyclic direct factors have order 2.

Problems 5C

5C.1. Show that Burnside's normal p -complement theorem is a consequence of Theorem 5.18.

5C.2. Suppose that $U \subseteq V \subseteq P \subseteq G$, where P is an abelian Sylow 2-subgroup of G and U and V are characteristic in P such that $|V : U| = 2$. If G is simple, show that $|G| = 2$.

5C.3. Let G be simple and have an abelian Sylow 2-subgroup P of order 2^5 . Deduce that P is elementary abelian.

5C.4. Suppose that all Sylow subgroups of G are cyclic. Show that for every divisor m of $|G|$, there exists a subgroup of order m , and show that every two subgroups of order m are conjugate in G .

5C.5. Let $P \in \text{Syl}_p(G)$ and suppose that A and B are G -conjugate normal subgroups of P . Show that A and B are conjugate in $\text{N}_G(P)$. If A is characteristic in P , deduce that $A = B$.

Note. If A is characteristic in $P \in \text{Syl}_p(G)$, it is certainly possible for A to be G -conjugate to some subgroup B of P with $B \neq A$. But among all G -conjugates B of A that are contained in P , the only one that can be normal in P is A itself.

5C.6. Let $W \subseteq H \subseteq G$. We say that W is **weakly closed** in H with respect to G if the only G -conjugate of W contained in H is W itself. Now suppose that $P \in \text{Syl}_p(G)$ and that $W \subseteq P$.

- (a) If W is weakly closed in P with respect to G , show that W is weakly closed in Q for each Sylow p -subgroup Q of G that contains W .
- (b) Show that W is weakly closed in P with respect to G if and only if W is normal in $\text{N}_G(P)$ and it is also normal in all Sylow p -subgroups of G that contain it.
- (c) Suppose that W is weakly closed in P with respect to G , and let $W \subseteq H \subseteq G$. Show that every G -conjugate of W contained in H is actually H -conjugate to W .
- (d) Suppose that $W \subseteq \mathbf{Z}(P)$ and that W is weakly closed in P with respect to G . Show that $\text{N}_G(W)$ controls G -fusion in P .

5C.7. Let $|G| = 3^a \cdot 5 \cdot 11$. Show that G has a normal Sylow 3-subgroup.

5C.8. Let $p > 2$ be the smallest prime divisor of $|G|$, and suppose that $|G|$ is not divisible by p^3 . Show that G has a normal p -complement.

5C.9. Suppose that G is nonabelian simple and has even order not divisible by 8. Show that $|G|$ is divisible by 3.

Note. There do exist nonabelian simple groups with order not divisible by 3, but all such groups have order divisible by 64. In fact, the only nonabelian simple $3'$ -groups are the Suzuki groups $Sz(q)$, where $q = 2^e$ and $e > 1$ is odd. The group $Sz(q)$ has order $q^2 \cdot (q - 1) \cdot (q^2 + 1)$.

5C.10. Suppose that G is simple and has an abelian Sylow 2-subgroup of order 8. Show that $|G|$ has order divisible by 7.

Note. The simple group $PSL(2, 8)$ of order $504 = 2^3 \cdot 3^2 \cdot 7$ has an elementary abelian Sylow 2-subgroup of order 8. The same is true for the smallest Janko sporadic simple group J_1 , which has order $175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$.

5C.11. Let H be a Hall subgroup of G , and assume that $H \subseteq \mathbf{Z}(\mathbf{N}_G(H))$. Show that G has a normal p -complement for every prime divisor p of $|H|$.

Hint. Work by induction on $|G|$. Show that if P is a Sylow p -subgroup of H and $\mathbf{N}_G(P) < G$, then P is central in $\mathbf{N}_G(P)$. If $P \triangleleft G$ and Q is a Sylow subgroup of H with $\mathbf{N}_G(Q) < G$, show that P is central in $\mathbf{N}_G(Q)$.

5C.12. Suppose that G has a cyclic Sylow p -subgroup, and let $N \triangleleft G$ have index divisible by p . Prove that N has a normal p -complement.

5C.13. (Navarro) Suppose that P is a Sylow subgroup of G such that $P = \mathbf{N}_G(P)$. Show that $\mathbf{N}_G(P')$ has a normal p -complement.

Hint. Without loss of generality, $P' \triangleleft G$. Show that G is p -solvable, and let X be a Hall p -subgroup. Show that $G = P'\mathbf{N}_G(X)$ and apply Dedekind's lemma.

5D

We have seen that transfer theory can sometimes be used to prove that a group is not simple, and as we saw in the previous section, the transfer into a Sylow p -subgroup may be sufficient to accomplish this, especially when the Sylow subgroup is abelian. We ask now, when does this work? In other words, if v is the transfer from G to a not necessarily abelian Sylow p -subgroup P of G , we want to know when it is true that $\ker(v) < G$. Since $G/\ker(v) \cong v(G) \subseteq P/P'$, we see that $G/\ker(v)$ is an abelian p -group, and hence transfer to a Sylow p -subgroup can prove nonsimplicity only for groups that have factor groups that are nontrivial abelian p -groups. One of the results we prove in this section is that if G actually has such a factor group, then this fact can definitely be established by considering the transfer to a Sylow p -subgroup.

In order to make a more precise statement, we introduce some notation. Given a prime p and a finite group G , let $\mathbf{A}^p(G)$ denote the unique smallest normal subgroup of G for which the corresponding factor group is an abelian p -group. (That $\mathbf{A}^p(G)$ is well defined is an immediate consequence of the fact that if $M, N \triangleleft G$ and both G/M and G/N are abelian p -groups, then $G/(M \cap N)$ is also an abelian p group.) There is, of course,

an obvious analogy between the definitions of $\mathbf{A}^p(G)$ and $\mathbf{O}^p(G)$, which, we recall, is the unique smallest normal subgroup of G whose factor group is a (not necessarily abelian) p -group. In fact, $\mathbf{A}^p(G)$ and $\mathbf{O}^p(G)$ are more intimately connected than merely by analogy. We have $\mathbf{O}^p(G) \subseteq \mathbf{A}^p(G)$ and $G/\mathbf{A}^p(G)$ is isomorphic to the largest abelian factor of $G/\mathbf{O}^p(G)$. Thus $\mathbf{A}^p(G)/\mathbf{O}^p(G) = (G/\mathbf{O}^p(G))' = G'\mathbf{O}^p(G)/\mathbf{O}^p(G)$, and therefore, $\mathbf{A}^p(G) = G'\mathbf{O}^p(G)$. Also, it should be clear that $\mathbf{A}^p(G)/G' = \mathbf{O}^p(G/G')$ is the normal p -complement of G/G' .

5.20. Theorem. *Let $v : G \rightarrow P/P'$ be the transfer homomorphism, where G is a finite group and $P \in \text{Syl}_p(G)$. Then $\ker(v) = \mathbf{A}^p(G)$.*

In the previous section, we were able to obtain results about the transfer from G into an abelian Sylow subgroup P because in that case, $\mathbf{N}_G(P)$ controls G -fusion in P . In order to study the general case, where P is not necessarily abelian, we need other techniques that help in the study of fusion, and so we make the following definition, which is the key to the proofs of Theorem 5.20 and other results in this section. If $H \subseteq G$ is an arbitrary subgroup, we define the **focal subgroup** of H with respect to G to be the subgroup generated by all elements of the form $x^{-1}y$, where x and y are G -conjugate elements of H . This subgroup is denoted $\text{Foc}_G(H)$.

If $x, h \in H$, then of course, x and x^h are G -conjugate elements of H (because they are H -conjugate), and so $x^{-1}x^h$ lies in $\text{Foc}_G(H)$. But $x^{-1}x^h = [x, h]$, and this shows that $\text{Foc}_G(H)$ contains all commutators of elements of H . It follows that $H' \subseteq \text{Foc}_G(H)$, and in fact, $H' = \text{Foc}_H(H)$. Now assume $x, y \in H$ are G -conjugate, so that $y = x^g$ for some element $g \in G$. Then $x^{-1}y = [x, g] \in G'$, and hence $\text{Foc}_G(H) \subseteq G'$. Finally, we recall that if $H \subseteq K \subseteq G$ and K controls G -fusion in H , then two elements $x, y \in H$ are G -conjugate if and only if they are K -conjugate. It follows in this case that $\text{Foc}_K(H)$ and $\text{Foc}_G(H)$ have exactly the same generating sets, and so $\text{Foc}_K(H) = \text{Foc}_G(H)$.

Throughout much of the rest of this chapter, our primary interest will be the transfer into a Sylow p -subgroup of G . Many of our arguments, however, would work as well for an arbitrary Hall π -subgroup, where π is a set of primes. The following “focal subgroup theorem”, for example, is valid for an arbitrary Hall π -subgroup, and the proof of the more general version goes through without change. The only extra work required is to define $\mathbf{A}^\pi(G)$ in the obvious way: it is the unique smallest normal subgroup of G for which the factor group is an abelian π -group.

5.21. Theorem (Focal Subgroup). *Suppose that P is a Sylow p -subgroup of a finite group G , and let $v : G \rightarrow P/P'$ be the transfer homomorphism.*

Then

$$\text{Foc}_G(P) = P \cap G' = P \cap \mathbf{A}^p(G) = P \cap \ker(v).$$

Proof. First, observe that

$$\text{Foc}_G(P) \subseteq P \cap G' \subseteq P \cap \mathbf{A}^p(G) \subseteq P \cap \ker(v).$$

The first of these containments holds because the focal subgroup $\text{Foc}_G(P)$ is contained in P by definition, and we observed previously that $\text{Foc}_G(P) \subseteq G'$. The second containment holds since $G/\mathbf{A}^p(G)$ is abelian, and so $G' \subseteq \mathbf{A}^p(G)$, and finally, the third containment holds because $G/\ker(v) \cong v(G) \subseteq P/P'$, which is an abelian p -group, and thus $\mathbf{A}^p(G) \subseteq \ker(v)$. To complete the proof, therefore, it suffices to show that $P \cap \ker(v) \subseteq \text{Foc}_G(P)$.

Let $x \in P \cap \ker(v)$, and let T_t be a right transversal for P in G . To apply the transfer-evaluation lemma to compute $v(x)$, we choose an appropriate subset $T_0 \subseteq T_t$ and positive integers n_t for $t \in T_0$. Then x^{n_t} and $tx^{n_t}t^{-1}$ are G -conjugate members of P , and thus

$$(x^{-n_t})(tx^{n_t}t^{-1}) \in \text{Foc}_G(P)$$

for all $t \in T_0$. It follows that the product of these elements (in any order) lies in $\text{Foc}_G(P)$. Also, because $P' \subseteq \text{Foc}_G(P)$, we can arbitrarily rearrange elements of P in this product to deduce that

$$\prod_{t \in T_0} x^{-n_t} \prod_{t \in T_0} tx^{n_t}t^{-1} \in \text{Foc}_G(P),$$

or equivalently,

$$\prod_{t \in T_0} tx^{n_t}t^{-1} \equiv \prod_{t \in T_0} x^{n_t} \pmod{\text{Foc}_G(P)}.$$

By the transfer-evaluation lemma, the product on the left is congruent modulo P' to $V(x)$, where V is a pretransfer map from G to P . Since $x \in \ker(v)$, we have $V(x) \in P'$, and thus this product lies in $P' \subseteq \text{Foc}_G(P)$. It follows that the product on the right also lies in $\text{Foc}_G(P)$. But $\sum n_t = |G : P|$, and this yields $x^{|G:P|} \in \text{Foc}_G(P)$. Since $|P|$ and $|G : P|$ are coprime, there exists an integer m such that $m|G : P| \equiv 1 \pmod{|P|}$, and therefore,

$$x = (x^{|G:P|})^m \in \text{Foc}_G(P),$$

as required. ■

Theorem 5.20 is an immediate consequence of the focal subgroup theorem.

Proof of Theorem 5.20. Write $K = \ker(v)$ and $A = \mathbf{A}^p(G)$, so that $A \subseteq K$, and our goal is to prove that equality holds here. Since $|G : K|$ and

$|G : A|$ are p -powers, it follows that $PK = G = PA$, and by the focal subgroup theorem (Theorem 5.21), we have $P \cap K = P \cap A$. Then

$$|G : K| = |P : P \cap K| = |P : P \cap A| = |G : A|,$$

and since $A \subseteq K$, it follows that $A = K$, as wanted. ■

Now fix a Sylow p -subgroup P of G . Let $P \subseteq H \subseteq G$, and let v and w , respectively, be the transfer homomorphisms from G and H to P/P' . We wish to compare the kernels $\mathbf{A}^p(G)$ and $\mathbf{A}^p(H)$ and the images $v(G)$ and $w(H)$ of these two transfer maps. Since $PA^p(G) = G$, we have $HA^p(G) = G$, and thus $H/(H \cap \mathbf{A}^p(G)) \cong G/\mathbf{A}^p(G)$ is an abelian p -group. It follows that $\mathbf{A}^p(H) \subseteq H \cap \mathbf{A}^p(G)$, and thus $|v(G)| = |G : \mathbf{A}^p(G)| \leq |H : \mathbf{A}^p(H)| = |w(H)|$. It should be clear that equality holds here if and only if $\mathbf{A}^p(H) = H \cap \mathbf{A}^p(G)$, and also if and only if $|G : \mathbf{A}^p(G)| = |H : \mathbf{A}^p(H)|$. If equality does hold, we say that H **controls p -transfer** in G . (Occasionally, we will neglect to mention the group G , and simply say that “ H controls p -transfer”.)

The point here is this. If we know that H controls p -transfer in G , and we also know that $\mathbf{A}^p(H) < H$, it follows that $\mathbf{A}^p(G) < G$, and so G is nonsimple (unless $|G| = p$). In other words, a result that guarantees that some subgroup H containing a Sylow p -subgroup of G controls p -transfer allows us to shift the burden of proving the existence of a nontrivial abelian p -factor group from G to the smaller group H .

As before, suppose that $P \subseteq H \subseteq G$, where $P \in \text{Syl}_p(G)$. One way to guarantee that H controls p -transfer in G is to show that H controls G -fusion in P . (But we stress that H can control transfer without controlling fusion.)

5.22. Corollary. *Let $P \in \text{Syl}_p(G)$, where G is a finite group, and suppose that $P \subseteq H \subseteq G$, where H is a subgroup that controls G -fusion in P . Then H controls p -transfer, and hence*

$$\mathbf{A}^p(H) = H \cap \mathbf{A}^p(G) \quad \text{and} \quad G/\mathbf{A}^p(G) \cong H/\mathbf{A}^p(H).$$

Proof. Let v and w , respectively, be the transfer maps from G and from H to P/P' . Our goal is to show that $|G : \ker(v)| = |H : \ker(w)|$, or equivalently (by two applications of Lemma 5.11) that $|P : P \cap \ker(v)| = |P : P \cap \ker(w)|$. But $P \cap \ker(v) = \text{Foc}_G(P)$ and $P \cap \ker(w) = \text{Foc}_H(P)$ by the focal subgroup theorem (5.21), and we have $\text{Foc}_G(P) = \text{Foc}_H(P)$ since we are assuming that H controls G -fusion in P . The result now follows. ■

5.23. Corollary. *Let G be a finite group, and suppose that $P \in \text{Syl}_p(G)$ is abelian. Then $\mathbf{N}_G(P)$ controls p -transfer.*

Proof. We know by Lemma 5.12 that $N_G(P)$ controls G -fusion in P . The result follows by the previous corollary. ■

In fact, a condition much weaker than that the Sylow p -subgroup P is abelian is sufficient to establish that $N_G(P)$ controls p -transfer. A theorem of P. Hall and H. Wielandt asserts that $N_G(P)$ controls p -transfer whenever P has nilpotence class less than p . (In other words, it suffices that P should not be too severely nonabelian.) Actually, the Hall-Wielandt theorem is stronger than we have just stated, and in Chapter 10, we present an even stronger result due to T. Yoshida.

It is not hard to deduce the Burnside normal p -complement theorem from Corollary 5.23, and in fact, the more general Theorem 5.18 follows fairly easily too. Another application of Corollary 5.22 is the following.

5.24. Theorem. *Let G be a finite simple group, and suppose that $H \subseteq G$ is a maximal subgroup. If H is nilpotent, then H is a p -group for some prime p .*

Proof. We derive a contradiction by assuming that p and q are distinct primes that divide $|H|$. Let $P \in \text{Syl}_p(H)$, and observe that $P \triangleleft H$ since H is nilpotent. Also, P is nontrivial, and P is not normal in G since G is simple. Then $H \subseteq N_G(P) < G$, and we have $H = N_G(P)$ by the maximality of H . We deduce that P is a full Sylow p -subgroup of G since otherwise, $P < S$ for some p -subgroup S of G , and thus $P < N_S(P) = S \cap N_G(P) = S \cap H$. This is impossible, however, since $S \cap H$ is a p -subgroup of H that properly contains the Sylow p -subgroup P of H .

Similarly, $H = N_G(Q)$, where $Q \in \text{Syl}_q(H)$, and we have $Q \in \text{Syl}_q(G)$. It follows by Lemma 5.12 applied to Q that $H = N_G(Q)$ controls G -fusion in $C_G(Q)$. But $P \subseteq C_G(Q)$ since P and Q are normal subgroups of H and $P \cap Q = 1$. We conclude that H controls G -fusion in P . Since $P \in \text{Syl}_p(G)$ and $H = N_G(P)$, we deduce from Corollary 5.22 that H controls p -transfer in G .

Now H is nilpotent and has order divisible by p , and thus $O^p(H) < H$. It follows that $A^p(H) < H$ because the nontrivial p -group $H/O^p(H)$ must have a nontrivial abelian homomorphic image. Since H controls p -transfer in G and $A^p(H) < H$, we have $A^p(G) < G$, and hence since G is simple, $A^p(G) = 1$. Then G is a p -group, and this is the desired contradiction since q divides $|G|$. ■

The obvious question at this point is whether or not a nonabelian simple group actually can have a maximal subgroup that is a p -group for some prime p . The answer is “yes”, but only if $p = 2$. The Sylow 2-subgroup of

the simple group $PSL(2, 17)$ of order $2^4 \cdot 3^2 \cdot 17$ is maximal, and the impossibility for odd primes is a consequence of Thompson's normal p -complement theorem, which we prove in Chapter 7.

We close this section with a brief discussion of Tate's theorem, which can be viewed as a kind of "supercharger" for transfer theory. Suppose that, as usual, we have $P \subseteq H \subseteq G$, where $P \in \text{Syl}_p(G)$. We have seen that under suitable hypotheses, it may be possible to show that H controls p -transfer, which, we recall, means that $\mathbf{A}^p(H) = H \cap \mathbf{A}^p(G)$. (We know, for example, that this happens if H controls G -fusion in P , and there are also other situations where control of p -transfer can be established.) Tate's theorem says that if $\mathbf{A}^p(H) = H \cap \mathbf{A}^p(G)$, then, in fact, $\mathbf{O}^p(H) = H \cap \mathbf{O}^p(G)$. (The converse of this is easy: if $\mathbf{O}^p(H) = H \cap \mathbf{O}^p(G)$, it is routine to show that $\mathbf{A}^p(H) = H \cap \mathbf{A}^p(G)$.)

In order to see the significance of Tate's theorem, we consider a special case. Suppose that in some group G , we have $G' \cap P = P'$, where $P \in \text{Syl}_p(G)$. Since $|\mathbf{A}^p(G) : G'|$ is a p' -number, it follows easily that $\mathbf{A}^p(G) \cap P = G' \cap P$, and thus $\mathbf{A}^p(G) \cap P = P' = \mathbf{A}^p(P)$. We can now apply Tate's theorem with $H = P$ to conclude that $\mathbf{O}^p(G) \cap P = \mathbf{O}^p(P) = 1$. It follows that $|\mathbf{O}^p(G)|$ is not divisible by p , and thus $\mathbf{O}^p(G)$ is a normal p -complement in G . To summarize, we have shown using Tate's theorem that if $G' \cap P = P'$, where $P \in \text{Syl}_p(G)$, then G must have a normal p -complement.

Unfortunately, we cannot prove Tate's theorem here. There seems to be no easy proof of this result, or even of the corollary that we discussed in the previous paragraph. Tate's original argument used cohomology theory, but we prefer Thompson's pretty character theoretic proof, which is presented in the author's character theory text.

Problems 5D

5D.1. Let $P \in \text{Syl}_p(G)$, where P is abelian. Let $P \subseteq H \subseteq G$, and assume that H controls p -transfer in G . If H has a normal p -complement, show that G has a normal p -complement.

5D.2. Let $P \in \text{Syl}_p(G)$ and assume that $P \subseteq \mathbf{Z}(G)$. Without using Burnside's normal p -complement theorem or any other part of transfer theory, deduce that G has a normal p -complement. Use this to derive Burnside's theorem from Corollary 5.23.

5D.3. Let G be a nonabelian simple group, and suppose that $P \subseteq G$ is a p -subgroup that is a maximal subgroup of G .

(a) Show that $P \in \text{Syl}_p(G)$.

- (b) If $1 < N \triangleleft P$ and P/N is abelian, show that P is the unique Sylow p -subgroup of G that contains N . Deduce that N is weakly closed in P with respect to G . (See Problem 5C.6.)
- (c) Show that the nilpotence class of P must be at least 3.

Hint. If P has class less than 3, apply (b) with $N = \mathbf{Z}(P)$, and use Problem 5C.6(d).

5D.4. Let $P \in \text{Syl}_p(G)$ and suppose that $P \subseteq K \subseteq G$. Show that $\mathbf{O}^p(K) \subseteq K \cap \mathbf{O}^p(G)$ and that if equality holds, then $\mathbf{A}^p(K) = K \cap \mathbf{A}^p(G)$.

5D.5. Suppose that $P \in \text{Syl}_p(G)$, and assume that $A \cap P = P'$, where $A = \mathbf{A}^p(G)$. If $P' \triangleleft A$, prove (without appealing to Tate's theorem) that G has a normal p -complement.

Hint. Using the Schur-Zassenhaus theorem, let K be a complement for P' in A and show that $G = \mathbf{N}_G(K)P'$. Using the fact that $P' \subseteq \Phi(P)$, deduce that P normalizes K .

5D.6. As in the previous problem, suppose that $P \in \text{Syl}_p(G)$, and assume that $A \cap P = P'$, where $A = \mathbf{A}^p(G)$. If P' is abelian, prove (without appealing to Tate's theorem) that G has a normal p -complement.

Hint. Let $N = \mathbf{N}_G(P')$ and observe that N satisfies the hypotheses. Use Burnside's normal p -complement theorem in the group A .

5E

We return now to the problem of determining when a finite group G has a normal p -complement. Of course, Burnside's theorem guarantees the existence of such a complement if $P \subseteq \mathbf{Z}(\mathbf{N}_G(P))$, where P is a Sylow p -subgroup of G . But since this hypothesis can only hold if P is abelian, Burnside's result tells us nothing if P is nonabelian. The focal subgroup theorem, however, can be used to establish a necessary and sufficient condition for G to have a normal p -complement, with no assumption that the Sylow subgroup is abelian.

5.25. Theorem. *A finite group G has a normal p -complement if and only if a Sylow p -subgroup of G controls its own fusion in G .*

Proof. First, assume that N is a normal p -complement in G , and let $P \in \text{Syl}_p(G)$. Then $NP = G$ and $N \cap P = 1$, and thus the restriction to P of the canonical homomorphism $G \rightarrow \overline{G} = G/N$ is an isomorphism of P onto G/N . Now suppose that $x, y \in P$ are conjugate in G . Then their images \bar{x} and \bar{y} are conjugate in \overline{G} , and it follows via the isomorphism $u \mapsto \bar{u}$ from P

to \overline{G} that x and y are conjugate in P . Thus P controls its own fusion in G , as required.

Conversely, assume that P controls its own fusion in G . Let $N = \mathbf{O}^p(G)$, and write $Q = N \cap P$, so that $Q \in \text{Syl}_p(N)$. We will show that N is a normal p -complement in G by proving that $Q = 1$. We argue first that $\mathbf{A}^p(N) = N$. To see why this is so, observe that $\mathbf{A}^p(N)$ is characteristic in N , and hence is normal in G . Furthermore,

$$|G : \mathbf{A}^p(N)| = |G : N| |N : \mathbf{A}^p(N)|,$$

which is a power of p , and thus $N = \mathbf{O}^p(G) \subseteq \mathbf{A}^p(N)$. It follows that $N = \mathbf{A}^p(N)$, as claimed. By the focal subgroup theorem, therefore, $\text{Foc}_N(Q) = Q \cap \mathbf{A}^p(N) = Q \cap N = Q$.

Now let $x, y \in Q$ be N -conjugate, so that $x^{-1}y$ is a typical generator for $\text{Foc}_N(Q)$. Then x and y are G -conjugate elements of P , and so by hypothesis, they are conjugate in P , and we can write $y = x^u$ with $u \in P$. We have $x^{-1}y = x^{-1}x^u = [x, u] \in [Q, P]$, and it follows that $\text{Foc}_N(Q) \subseteq [Q, P]$. Since $\text{Foc}_N(Q) = Q$, we have $Q \subseteq [Q, P]$, and thus $Q \subseteq [Q, P, P, \dots, P]$, where there are arbitrarily many commutations with P . But P is nilpotent and $Q \subseteq P$, and thus with sufficiently many commutations, we have $[Q, P, P, \dots, P] = 1$. It follows that $Q = 1$, and so N is a normal p -complement in G , as wanted. ■

Although it is pleasant that Theorem 5.25 gives a necessary and sufficient condition for G to have a normal p -complement, this result is of limited applicability because in general, it is difficult to determine whether or not a Sylow p -subgroup of G controls its own fusion. A deeper and much more useful criterion for G to have a normal p -complement is the following result of Frobenius, which shows that the existence of a normal p -complement in G is determined by the p -local subgroups of G . (Recall that a subgroup $N \subseteq G$ is said to be p -local in G if $N = \mathbf{N}_G(X)$, where X is some nonidentity p -subgroup of G .)

5.26. Theorem (Frobenius). *Let G be a finite group, and suppose p is a prime. Then the following are equivalent.*

- (1) G has a normal p -complement.
- (2) $\mathbf{N}_G(X)$ has a normal p -complement for every nonidentity p -subgroup $X \subseteq G$.
- (3) $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group for every p -subgroup $X \subseteq G$.

Observe that if we were to drop the word “nonidentity” from assertion (2), the theorem would still be true, but it would be far less interesting. This is so because if $X = 1$, then $\mathbf{N}_G(X) = G$, and the implication (2) \Rightarrow (1)

would have no content. On the other hand, assertion (3) is automatically true when $X = 1$, and hence it is irrelevant whether or not we restrict (3) to nonidentity subgroups X . (We have chosen not to include such a restriction.) Also, we stress that in general, it is not true that if $X \subseteq G$ is a p -subgroup and $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group, then $\mathbf{N}_G(X)$ has a normal p -complement. The theorem tells us that if for *every* p -subgroup $X \subseteq G$, it is true that $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group, then it is also true that $\mathbf{N}_G(X)$ has a normal p -complement for every p -subgroup $X \subseteq G$. The implication (3) \Rightarrow (2) is not valid for individual p -subgroups X , however.

The implications (1) \Rightarrow (2) \Rightarrow (3) of Frobenius' theorem are nearly trivial, and we dispose of them first.

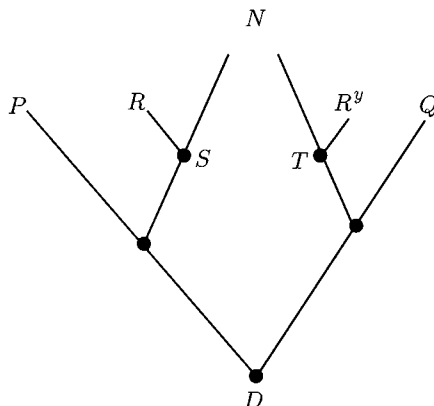
5.27. Lemma. *In the situation of Theorem 5.26, if (1) holds, then so does (2), and if (2) holds, then so does (3).*

Proof. To prove that (1) \Rightarrow (2), we show more: if G has a normal p -complement, then every subgroup $H \subseteq G$ has a normal p -complement. To see this, suppose that N is a normal p -complement in G . Then $N \cap H$ is a normal subgroup of H having p' -order, and since $|H : H \cap N| = |NH : N|$ divides $|G : N|$, which is a p -power, it follows that $N \cap H$ is actually a normal p -complement in H , as wanted.

Now assume (2), and let $X \subseteq G$ be a p -subgroup. If $X = 1$, then $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is trivial, and so is a p -group, as required. Otherwise, we know that $\mathbf{N}_G(X)$ has a normal p -complement K , and we see that K centralizes X since $X \cap K = 1$ and both X and K are normal subgroups of $\mathbf{N}_G(X)$. Then $K \subseteq \mathbf{C}_G(X)$, and so $|\mathbf{N}_G(X) : \mathbf{C}_G(X)|$ divides $|\mathbf{N}_G(X) : K|$, which is a power of p . Thus $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group, as required. ■

The key to the proof of Frobenius' theorem is the following.

5.28. Lemma. *Assume that $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group for every p -subgroup X of a finite group G , and let $P, Q \in \text{Syl}_p(G)$. Then $Q = P^c$, for some element $c \in \mathbf{C}_G(P \cap Q)$.*



Proof. Let \mathcal{P} be the set of pairs (P, Q) , where $P, Q \in \text{Syl}_p(G)$ are not necessarily distinct, and such that $Q = P^c$ for some element $c \in \mathbf{C}_G(P \cap Q)$. Our goal, of course, is to show that the set \mathcal{P} consists of all pairs of members of $\text{Syl}_p(G)$. If this is false, choose $P, Q \in \text{Syl}_p(G)$ with $P \cap Q$ as large as possible such that $(P, Q) \notin \mathcal{P}$. Write $D = P \cap Q$, and observe that $D < P$ and $D < Q$, since otherwise $P = D = Q$, and thus (P, Q) lies in \mathcal{P} since we can take $c = 1$.

Let $N = \mathbf{N}_G(D)$. Since $P \cap N$ and $Q \cap N$ are p -subgroups of N , they are contained in Sylow p -subgroups S and T of N , respectively, and S is contained in some Sylow p -subgroup R , of G as shown in the diagram. Let $C = \mathbf{C}_G(D)$, so that N/C is a p -group by hypothesis. Then $N = SC$ since S is a Sylow p -subgroup of N . By the Sylow C -theorem, $T = S^n$ for some element $n \in N$, and we can write $n = sy$, where $s \in S$ and $y \in C$. Then $T = S^n = S^{sy} = S^y$, and since $S \subseteq R$, it follows that $T = S^y \subseteq R^y$.

Now $P \cap N \subseteq S \subseteq R$, and so $P \cap N \subseteq P \cap R$. But $P \cap N = \mathbf{N}_P(D) > D$ since $D < P$ and “normalizers grow” in p -groups. We conclude that $P \cap R > D = P \cap Q$, and so by the choice of P and Q , we have $(P, R) \in \mathcal{P}$. We can thus write $R = P^x$ for some element $x \in \mathbf{C}_G(P \cap R)$, and in particular, we observe that x centralizes D . Also, $Q \cap N \subseteq T \subseteq R^y$, and thus $Q \cap N \subseteq R^y \cap Q$. But $Q \cap N = \mathbf{N}_Q(D) > D$ since $D < Q$, and thus $R^y \cap Q > D = P \cap Q$. Again by the choice of P and Q , we have $(R^y, Q) \in \mathcal{P}$, and we can write $Q = (R^y)^z$ for some element $z \in \mathbf{C}_G(R^y \cap Q)$, and so in particular, z centralizes D . Now $P^{xyz} = R^{yz} = Q$, and since each of x , y and z centralizes D , it follows that xyz centralizes D , and thus (P, Q) lies in \mathcal{P} , which is a contradiction. ■

Proof of Theorem 5.26. By Lemma 5.27, it suffices to prove that (3) \Rightarrow (1), and so we assume (3), and we show that G has a normal p -complement. By Theorem 5.25, it is enough to prove that a Sylow p -subgroup P of G controls its own fusion in G . We therefore assume that $x, y \in P$ are conjugate in G , and we work to show that x and y are actually conjugate in P .

Write $y = x^g$ with $g \in G$, and observe that $y \in P \cap P^g$. By Lemma 5.28, there is an element $c \in \mathbf{C}_G(P \cap P^g)$ such that $(P^g)^c = P$, and we see that c centralizes y . By hypothesis, $\mathbf{N}_G(P)/\mathbf{C}_G(P)$ is a p -group, and since P

is a Sylow p -subgroup of $\mathbf{N}_G(P)$, we can write $\mathbf{N}_G(P) = \mathbf{C}_G(P)P$. We have $gc \in \mathbf{N}_G(P)$, and so we can write $gc = tu$, where $t \in \mathbf{C}_G(P)$ and $u \in P$. In particular, since $x \in P$, we see that t centralizes x , and thus $y = y^c = x^{gc} = x^{tu} = x^u$. Since $u \in P$, it follows that x and y are conjugate in P , as required. This completes the proof. ■

How can we check that $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group for some p -group X ? This is equivalent to saying that $\mathbf{C}_G(X)$ contains a full Sylow q -subgroup of $\mathbf{N}_G(X)$ for every prime q different from p . In other words, a group G satisfies (3) of Frobenius' theorem if whenever a g -subgroup Q of G acts on (normalizes) a p -subgroup X of G , the action is trivial. This yields the following corollary.

5.29. Corollary. *Suppose G is a finite group and $|G| = p^a m$, where p does not divide m . Assume that no prime divisor q of m divides an integer of the form $p^e - 1$, where $1 \leq e \leq a$. Then G has a normal p -complement.*

It follows, for example, that every nonabelian simple group of even order either has order divisible by 32, or by one of 3, 5 or 7. To see why this is so, write $|G| = 2^a m$, where m is odd, and suppose that $a < 5$. Since G is nonabelian and simple and has even order, it does not have a normal 2-complement. By Corollary 5.29, therefore, m cannot be coprime to all of the numbers $2^e - 1$, where $1 \leq e \leq 4$. Since $2^1 - 1 = 1$, $2^2 - 1 = 3$, $2^3 - 1 = 7$ and $2^4 - 1 = 15$, at least one of the primes 3, 5 or 7 must divide m .

Of course, by the Feit-Thompson odd-order theorem, every nonabelian simple group has even order. Also, it follows from the classification of simple groups that the order of every such group is divisible by 3 or 5.

Proof of Corollary 5.29. If G does not have a normal p -complement, then (3) of Frobenius' theorem must fail, and thus G contains a g -subgroup Q that acts nontrivially on some p -subgroup X , where q is some prime divisor of m . Now $\mathbf{C}_X(Q) < X$, so we can write $|X : \mathbf{C}_X(Q)| = p^e$, where $1 \leq e \leq a$. All of the elements of $X - \mathbf{C}_X(Q)$ lie in Q -orbits of size divisible by q , and it follows that q divides $|X| - |\mathbf{C}_X(Q)| = |\mathbf{C}_X(Q)|(p^e - 1)$. But $|\mathbf{C}_X(Q)|$ is a power of p and hence is coprime to q , and thus q divides $p^e - 1$. The result now follows. ■

A somewhat less trivial application is the following.

5.30. Corollary. *Let p be an odd prime, and suppose that every element of order p in the finite group G is central. Then G has a normal p -complement.*

Proof. Otherwise, G has a p -subgroup X acted on nontrivially by a q -subgroup Q , where q is some prime different from p . Since the elements of

order p in X are central in G , all of them are fixed by Q , and it follows by Theorem 4.36 that Q acts trivially on X . This is a contradiction. ■

Although Corollary 5.30 fails for $p = 2$, it is true that G has a normal 2-complement if every element $x \in G$ such that $x^4 = 1$ is central in G . The proof of this is essentially the same as that of Corollary 5.30, except that one must appeal to Problem 4D.4 in place of Theorem 4.36.

We mention that if $p > 2$, there is a much stronger version of the implication $(2) \Rightarrow (1)$ in Frobenius' theorem. In order to show that G has a normal p -complement, it is not necessary to check that $\mathbf{N}_G(X)$ has a normal p -complement for every nonidentity p -subgroup X of G . In fact, it suffices to consider just *two* such subgroups: the center $\mathbf{Z}(P)$, and a certain characteristic subgroup $\mathbf{J}(P)$, where $P \in \text{Syl}_p(G)$. This theorem of Thompson is proved in Chapter 7.

Problems 5E

5E.1. Let G be finite, and suppose that every proper subgroup of G has a normal p -complement but that G itself does not. Show that G has a normal Sylow p -subgroup and that $|G|$ has exactly one prime divisor other than p .

5E.2. Let G be a finite group in which every proper subgroup is supersolvable. Show that G is solvable.

Hint. If G is a counterexample of minimal order, show that G is simple. Then use Problem 3B.10 to show that G must have a normal p -complement, where p is the smallest prime divisor of $|G|$.

5E.3. Suppose that every two-generator subgroup of a finite group G has a normal p -complement. Show that G has a normal p -complement.

Hint. Consider $\langle x, y \rangle$, where x lies in some p -subgroup P and $y \in \mathbf{N}_G(P)$ has order not divisible by p .

Frobenius Actions

6A

Let A and N be finite groups, and suppose that A acts on N via automorphisms. The action of A on N is said to be **Frobenius** if $n^a \neq n$ whenever $n \in N$ and $a \in A$ are nonidentity elements. Equivalently, the action of A on N is Frobenius if and only if $C_N(a) = 1$ for all nonidentity elements $a \in A$, and also if and only if $C_A(n) = 1$ for all nonidentity elements $n \in N$. Yet another point of view is to consider the orbits of the action of A on the elements of N . If $1 \neq n \in N$, then by the fundamental counting principle, the size of the A -orbit of n is $|A : C_A(n)|$, and so we see that the action is Frobenius if and only if all A -orbits on N other than the trivial orbit $\{1\}$ have size equal to $|A|$. (Recall that an orbit of an action of a finite group A on some set is said to be regular if the orbit size is equal to $|A|$. If all A -orbits are regular, the action is **semiregular**.) Thus an action via automorphisms of A on N is Frobenius precisely when A acts semiregularly on the nonidentity elements of N . Finally, to conclude this introduction to Frobenius actions, we observe that if A acts on N via automorphisms and the action is Frobenius, then the natural action of every subgroup of A on N is also Frobenius, and so is the action of A on every subgroup of N that admits A .

By the following easy observation, Frobenius actions are automatically coprime actions. Everything we know about coprime actions from Chapter 3, therefore, applies to Frobenius actions.

6.1. Lemma. *Let A and N be finite groups, and suppose there is a Frobenius action of A on N . Then $|N| \equiv 1 \pmod{|A|}$, and hence $|N|$ and $|A|$ are coprime.*

Proof. The set N is decomposed into A -orbits. One of these is $\{1\}$ and all of the others are regular orbits, which have size $|A|$. The result follows. ■

6.2. Corollary. *Let A and N be finite groups, and suppose there is a Frobenius action of A on N . Let M be an A -invariant normal subgroup of N . Then the induced action of A on N/M is Frobenius.*

Proof. Let $1 \neq a \in A$. Then $\langle a \rangle$ acts coprimely on N , and we recall from Corollary 3.28 and the discussion preceding it that in coprime actions, “fixed points come from fixed points” in the induced action on the factor group $N/M = \overline{N}$. (This assumes that one of $\langle a \rangle$ or M is solvable, but since $\langle a \rangle$ is cyclic, this hypothesis is satisfied.) It follows that $\mathbf{C}_{\overline{N}}(\langle a \rangle) = \overline{\mathbf{C}_N(\langle a \rangle)}$, and this is trivial since $\mathbf{C}_N(\langle a \rangle) = 1$. Thus $\mathbf{C}_{\overline{N}}(a) = 1$, and so the action of A on \overline{N} is Frobenius, as required. ■

Before we proceed to develop the theory of Frobenius actions, it seems appropriate to discuss some examples. Of course, if either A or N is the trivial group, then the unique (but not very interesting) action of A on N is Frobenius, but it is almost as easy to construct some nontrivial Frobenius actions. For example, if A has order 2 with nonidentity element a , and N is abelian of odd order, we can define a Frobenius action of A on N by setting $n^a = n^{-1}$ for all $n \in N$.

Next, consider a finite field F of order q . Let N be the additive group of F , and let A be a subgroup of the multiplicative group $F^\times = F - \{0\}$ of F . Thus N is an elementary abelian p -group, where p is the unique prime divisor of q , and since F^\times is cyclic of order $q - 1$, we can take A to be cyclic of order r for an arbitrary divisor r of $q - 1$. If $n \in N$ and $a \in A$, we define an action by setting $n^a = na$, where the product na is defined by viewing both n and a as elements of F and using the field multiplication. This really is an action via automorphisms since if $x, y \in N$, then $(x + y)^a = (x + y)a = xa + ya = x^a + y^a$ by the distributive law. To see that this action is Frobenius, suppose that $n^a = n$. Then $na = n$, and so $n(a - 1) = 0$. It follows that either $n = 0$, which is the identity in N , or $a = 1$, which is the identity in A .

Given primes p and r , let N and A , respectively, have orders p and r . By the construction of the previous paragraph, we see that there is a Frobenius action of A on N provided that r divides $p - 1$. (Of course, this divisibility condition is necessary by Lemma 6.1.) In fact, an arbitrary nontrivial action of a group A of prime order r on a group N of prime order p is necessarily Frobenius since if $n \in N$ and $a \in A$ are nonidentity elements, then a cannot centralize n or else $A = \langle a \rangle$ centralizes $N = \langle n \rangle$, and the action is trivial. In particular, if the action of A on N is nontrivial, then r must divide $p - 1$ by Lemma 6.1.

Not every group A can have a Frobenius action on a nontrivial group N , and not every group N can admit a Frobenius action of a nontrivial group A . An easy result of this type is the following, but as we shall see after we develop the necessary machinery, much more is true.

6.3. Theorem. *Let A and N be finite groups, and suppose there is a Frobenius action of A on N . Assume that $|A|$ is even and that N is nontrivial. Then A contains a unique involution, and N is abelian.*

Proof. Since $|A|$ is even by assumption, we can fix some involution $t \in A$, and we consider the map $x \mapsto x^{-1}x^t$ from N to itself. If $x, y \in N$ and $x^{-1}x^t = y^{-1}y^t$, then $yx^{-1} = y^t(x^t)^{-1} = (yx^{-1})^t$. Since the action of A is Frobenius and $t \neq 1$, it follows that $yx^{-1} = 1$, and thus $x = y$. This shows that our map $x \mapsto x^{-1}x^t$ is injective, and hence it is also surjective because N is finite. Given an arbitrary element $y \in N$, therefore, we can write $y = x^{-1}x^t$ for some element $x \in N$. Thus

$$y^t = (x^{-1}x^t)^t = (x^{-1})^t x = (x^t)^{-1} x = (x^{-1}x^t)^{-1} = y^{-1},$$

where the second equality holds since $t^2 = 1$. If $s \in A$ is an arbitrary involution, a similar calculation yields $y^s = y^{-1}$, and thus $y^s = y^t$. Then $y^{st^{-1}} = y$ for all $y \in N$, and since N is nontrivial by assumption, we can assume that $y \neq 1$, and thus $st^{-1} = 1$ because the action of A is Frobenius. Thus $s = t$, and hence t is the unique involution in A , as required.

We have seen that t inverts every element of N , and thus if $x, y \in N$, then $(xy)^t = (xy)^{-1} = y^{-1}x^{-1} = y^t x^t = (yx)^t$. It follows that $xy = yx$, and thus N is abelian. ■

A finite group A is said to be a **Frobenius complement** if it has a Frobenius action on some nonidentity group N , and similarly, a finite group N is a **Frobenius kernel** if it admits a Frobenius action by some nonidentity finite group A . (Our definition of “Frobenius complement” is not quite standard, but as we explain later, it is equivalent to the usual definition.) By Theorem 6.3, we know that a Frobenius complement of even order contains a unique involution, and we will prove that a Frobenius complement of odd order is even more tightly constrained. An odd order Frobenius complement, for example, contains a unique subgroup of order p for every prime p dividing its order.

There are also strong structural constraints on Frobenius kernels, as is suggested by the fact that the Frobenius kernel in Theorem 6.3 is abelian. In general, Frobenius kernels need not be abelian, but they are always nilpotent. The nilpotence of Frobenius kernels had been a long open problem, which was finally settled by J. Thompson in his Ph.D. thesis in 1959. We start work toward a proof of Thompson’s theorem in this chapter, and we

complete the proof in Chapter 7, where we present one of the key ingredients: Thompson's deep normal p -complement theorem.

All of the Frobenius complements and Frobenius kernels that we have seen so far are abelian, and in fact, all of our Frobenius complements have been cyclic. (We shall see that an abelian Frobenius complement is necessarily cyclic.) But nonabelian examples of Frobenius complements and kernels exist too. First, to show that a Frobenius kernel can be nonabelian, let F be a finite field of order q , and let N be the group of "unitary" upper triangular 3×3 matrices over F . (The elements of N are all of the 3×3 matrices over F with ones on the diagonal and zeros below the diagonal.) It should be clear that $|N| = q^3$, and it is easy to check that N is not abelian. If $q - 1$ is not a power of 2, we show that N is a Frobenius kernel by constructing a nonidentity subgroup A of the group $GL(3, F)$ of all invertible 3×3 matrices over F such that A acts by conjugation on N , and we will show that this action is Frobenius. (Note that although N is not abelian, it is nilpotent, as is required by Thompson's theorem.)

Let C be a (necessarily cyclic) odd-order subgroup of the multiplicative group F^\times of F , and let A be the group of 3×3 diagonal matrices of the form $a = \text{diag}(1, c, c^2)$, where c runs over C . (Note that we can choose C so that $|C|$ is an arbitrary odd divisor of $|F^\times| = q - 1$, and so, in particular, if $q - 1$ is not a power of 2, we can suppose that A is nontrivial.)

It is easy to check that A acts by conjugation on N , and that in fact,

$$\begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}^a = \begin{bmatrix} 1 & cx & c^2z \\ 0 & 1 & cy \\ 0 & 0 & 1 \end{bmatrix},$$

where $a = \text{diag}(1, c, c^2)$. If a is a nonidentity element of A , then $c \neq 1$, and thus also $c^2 \neq 1$ because we are assuming that C has odd order. If $n^a = n$ in this situation, we see that each of the above-diagonal entries x , y and z of n must be zero, and thus $n = 1$. It follows that the action is Frobenius.

Next, we mention some examples of nonabelian Frobenius complements. First, consider the group $S = SL(2, 3)$ of 2×2 matrices with determinant 1 over the field of order 3. It is easy to see that $|S| = 24$, and it is not hard to check that S has a unique Sylow 2-subgroup, which we will call Q . Of course, $|Q| = 8$, and in fact, Q is isomorphic to the quaternion group Q_8 . In particular, Q is noncyclic, and its unique element of order 2 is the negative of the identity matrix. Since Q is a subgroup of $SL(2, 3)$, it has a natural action on the vector space V of dimension 2 over the field of order 3, and since the unique element of order 2 in Q fixes no nonzero vector, it follows that the action of Q on the additive group of V is Frobenius. (Note that

since $|V| = 1 + |Q|$, the action of Q on the nonidentity elements of V is regular, and not just semiregular.)

Next, we appeal to the not completely obvious fact that $SL(2, 5)$ contains an isomorphic copy S of $SL(2, 3)$. (In fact, S is the normalizer in $SL(2, 5)$ of a Sylow 2-subgroup.) Since $S \subseteq SL(2, 5)$, there is an action of S on a 2-dimensional vector space W over a field of order 5, and it is easy to see that no element of order 2 or order 3 in $SL(2, 5)$ can have an eigenvalue equal to 1. No such element, therefore, can have a nontrivial fixed point on W , and it follows that the action of S on W is Frobenius. (Note that in this case too, the action on nonidentity elements is regular and not just semiregular since $|W| = 25 = 1 + 24 = 1 + |S|$.) Somewhat similarly, the group $SL(2, 5)$ can be embedded in $SL(2, 11)$, and this yields a Frobenius action of $SL(2, 5)$ on a vector space of order $11^2 = 121$. (Since $|SL(2, 5)| = 120$, we again have a regular action on nonidentity elements.) But $SL(2, 11)$ is not a Frobenius complement, and so the story ends here. (In fact, $SL(2, 11)$ contains a nonabelian subgroup of order 55, but we will prove that no Frobenius complement can have a noncyclic subgroup whose order is a product of two primes.)

Notice that the Frobenius complement $SL(2, 5)$ is not solvable. In fact, $SL(2, 5)$ is perfect, which, we recall, means that it is its own derived subgroup. A theorem of H. Zassenhaus asserts that $SL(2, 5)$ is the only perfect Frobenius complement. (We mention that one of the few serious errors in W. Burnside's classic group theory book is his assertion that Frobenius complements are always nilpotent. This false statement is his Theorem V on Page 336 of the 1911 edition.)

Next, we consider the semidirect product $G = N \rtimes A$, where A acts on N , and we ask what can be said about G if the given action is Frobenius. As usual when we consider semidirect products, we view N and A as subgroups of G , where N is normal and A is a complement for N in G . (Recall that this means that $NA = G$ and $N \cap A = 1$.) In this situation, of course, the original action of A on N is exactly the conjugation action of A on N in G .

6.4. Theorem. *Let N be a normal subgroup of a finite group G , and suppose that A is a complement for N in G . The following are then equivalent.*

- (1) *The conjugation action of A on N is Frobenius.*
- (2) *$A \cap A^g = 1$ for all elements $g \in G - A$.*
- (3) *$C_G(a) \subseteq A$ for all nonidentity elements $a \in A$.*
- (4) *$C_G(n) \subseteq N$ for all nonidentity elements $n \in N$.*

If both N and A are nontrivial in the situation of Theorem 6.4, we say that G is a **Frobenius group** and that A and N are respectively the Frobenius complement and Frobenius kernel of G .

We need the following easy computation.

6.5. Lemma. *Let A be a subgroup of a finite group G , and suppose that $A \cap A^g = 1$ for all elements $g \in G - A$. Let X be the subset of G consisting of those elements that are not conjugate in G to any nonidentity element of A . Then $|X| = |G|/|A|$.*

Proof. If $A = 1$, then A has no nonidentity elements, and so $X = G$ and there is nothing further to prove. Assuming that $A > 1$, we see that $A = N_G(A)$ since if $A^x = A$, then $A \cap A^x = A > 1$, and thus $x \in A$. It follows that A has exactly $|G : A|$ distinct conjugates in G . Furthermore, since each of these conjugates satisfies the condition we assumed about A , no two of them can have a nontrivial intersection. The conjugates of A , therefore, account for a total of $|G : A|(|A| - 1)$ nonidentity elements of G , and these are exactly the elements of G that are conjugate to nonidentity elements of A . We conclude that $|X| = |G| - |G : A|(|A| - 1) = |G : A|$, as required. ■

6.6. Corollary. *Let N be a normal subgroup of a finite group G , and suppose that A is a complement for N in G such that $A \cap A^g = 1$ for all elements $g \in G - A$. Then N is exactly the set X of Lemma 6.5. It is, in other words, the set of elements of G that are not conjugate to any nonidentity element of A .*

Proof. Since $N \cap A = 1$, it is also true that $N \cap A^g = 1$ for all $g \in G$, and thus no element of N can be conjugate to a nonidentity element of A . It follows that $N \subseteq X$. By Lemma 6.5, however, $|X| = |G|/|A| = |N|$, and the result follows. ■

In fact, the set X of Lemma 6.5 is *always* a subgroup. This remarkable theorem of Frobenius was proved using character theory, and no one has ever found a character-free proof. (We mention that it was Frobenius who invented character theory, and his proof that the set X is a subgroup is one of its earliest applications.) Observe that once we know that X is a subgroup, it is immediate that it is a normal subgroup. Also, by the definition of X , we know that $X \cap A = 1$, and so given that X is a subgroup, it follows by Lemma 6.5 that $|XA| = |X||A| = |G|$, and thus A complements the normal subgroup X in G . In other words, we are in the situation of Theorem 6.4, and condition (2) of that theorem holds. It follows that (1) holds, and so the conjugation action of A on X is Frobenius. In particular, if $A < G$, then A is a Frobenius complement in G . (Of course, the assumption that A is

proper is needed to guarantee that the group X is nontrivial.) Assuming Frobenius' theorem, therefore, we have shown that a subgroup $A < G$ is a Frobenius complement in G if and only if $A \cap A^g = 1$ for all elements $g \in G - A$. In fact, many authors use this as the definition of a Frobenius complement. (And indeed, we presented this definition in the note following problem 1D.3.)

Another way to think about Frobenius' theorem is this. Suppose that G acts transitively on some set Ω , and assume that no nonidentity element of G fixes as many as two members of Ω . Let $\alpha \in \Omega$, and let $A = G_\alpha$, the stabilizer of α . Now suppose that $g \in G - A$, and write $\beta = \alpha \cdot g$, so that $\beta \neq \alpha$. Then $A^g = G_\beta$, and so every element of $A \cap A^g$ fixes both α and β . By assumption, therefore, $A \cap A^g = 1$, and thus the point stabilizer $A = G_\alpha$ satisfies the hypothesis of Lemma 6.5. The elements of G conjugate to nonidentity elements of A are exactly the nonidentity elements of G that fix some point of Ω , and so in this context, the set X of Lemma 6.5 consists exactly of the identity together with those elements of G that fix no point of Ω . Frobenius' theorem tells us, therefore, that if G acts transitively on a set Ω and no nonidentity element of G fixes as many as two points, then the set consisting of the identity and the elements of G that fix no points forms a subgroup. In fact, it is not hard to see that this assertion about group actions is equivalent to Frobenius' theorem.

Proof of Theorem 6.4. Assume (1). To prove (2), suppose that $A \cap A^x > 1$ for some element $x \in G$. We work to show that $x \in A$. Since $G = AN$, we can write $x = an$ with $a \in A$ and $n \in N$, and thus $A^x = A^{an} = A^n$. Then $A^n \cap A > 1$, and so we can choose a nonidentity element b^n of this intersection, where $b^n \in A$ and $b \in A$. We thus have $[b, n] = b^{-1}b^n \in A$, and since $N \triangleleft G$, we also have $[b, n] \in N$. Then $[b, n] \in A \cap N = 1$, and hence b centralizes n . But the action of A on N is Frobenius by (1) and $b \neq 1$, and it follows that $n = 1$. Thus $x = an = a$ lies in A , as required.

Now assume (2), and let $1 \neq a \in A$. If $x \in \mathbf{C}_G(A)$, then $a \in A \cap A^x$, and since this intersection is nontrivial, it follows by (2) that $x \in A$. Thus $\mathbf{C}_G(a) \subseteq A$, proving (3).

Next, we show that (3) \Rightarrow (1). If $1 \neq a \in A$, then by (3), we have $\mathbf{C}_N(a) = N \cap \mathbf{C}_G(a) \subseteq N \cap A = 1$, and thus the action of A on N is Frobenius, which is assertion (1). We have now established that (1), (2) and (3) are equivalent.

Assuming (1) and (2) now, we prove (4) by showing that if $n \in N$ and $\mathbf{C}_G(n) \not\subseteq N$, then $n = 1$. By (2) and Corollary 6.6, we know that every element of G outside of N lies in some conjugate of A , and it follows that some nonidentity element of $\mathbf{C}_G(n)$ lies in a conjugate of A . For an

appropriate conjugate m of n , therefore, some nonidentity element of $\mathbf{C}_G(m)$ lies in A . Since $m \in N$ and the action of A on N is assumed to be Frobenius, it follows that $m = 1$, and thus $n = 1$, proving (4).

Finally, assuming (4), let $1 \neq n \in N$. Then $\mathbf{C}_A(n) = A \cap \mathbf{C}_G(n) \subseteq A \cap N = 1$, and thus the action of A on N is Frobenius, proving (1). ■

In fact, the overall assumption in Theorem 6.4 that G has a normal subgroup N complemented by a subgroup A is not entirely necessary. By Frobenius' theorem, condition (2), which concerns the embedding of A in G , guarantees the existence of the normal subgroup N for which A is a complement. Somewhat analogously, condition (4), which concerns the embedding of N in G , guarantees the existence of the complement A for N . This result, however, is far more elementary than Frobenius' theorem.

6.7. Theorem. *Let $N \triangleleft G$, where G is a finite group, and suppose $\mathbf{C}_G(n) \subseteq N$ for every nonidentity element $n \in N$. Then N is complemented in G , and if $1 < N < G$, then G is a Frobenius group with kernel N .*

Proof. Let p be a prime divisor of $|N|$. Choose $P \in \text{Syl}_p(N)$ and $S \in \text{Syl}_p(G)$, with $P \subseteq S$. Then $\mathbf{Z}(S) \subseteq \mathbf{C}_G(P)$, and since P is nontrivial and is contained in N , it follows by hypothesis that $\mathbf{C}_G(P) \subseteq N$, and thus $\mathbf{Z}(S) \subseteq N$. Now S is nontrivial and hence $\mathbf{Z}(S)$ is a nontrivial subgroup of N . By hypothesis, therefore, $S \subseteq \mathbf{C}_G(\mathbf{Z}(S)) \subseteq N$. Thus N contains a full Sylow p -subgroup of G for every prime p dividing $|N|$, and it follows that no such prime divides $|G : N|$. This shows that N is a normal Hall subgroup of G , and hence it has a complement A in G by the Schur-Zassenhaus theorem. If $1 < N < G$ then both N and A are nontrivial, and so G is a Frobenius group by Theorem 6.4. ■

Problems 6A

6A.1. Let A be a subgroup of $SL(2, p)$ of order not divisible by the prime p . Show that the action of A on the vector space of order p^2 is Frobenius.

6A.2. In the multiplicative group F^\times of a field F of order 43, let α have order 7 and let ϵ have order 3. Working in the group $GL(3, 43)$, let

$$a = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^4 & 0 \\ 0 & 0 & \alpha^2 \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \epsilon & 0 & 0 \end{bmatrix}.$$

Show that $A = \langle a, b \rangle$ is noncyclic of order 63, and that its natural action on the vector space V of order 43^3 is Frobenius.

Hint. Check that $\langle b \rangle$ has order 9 and normalizes $\langle a \rangle$, which has order 7. Also, observe that to show that the action is Frobenius, it suffices to check that $C_V(t) = 1$ for elements $t \in A$ of prime order.

Note. This problem shows that a nonabelian group of odd order can be a Frobenius complement.

6A.3. Show that there is a noncyclic group of order $5^2 \cdot 11$ that has a Frobenius action on some nontrivial group.

Hint. Work in $GL(5, p)$ for some appropriate prime p .

6A.4. Let G be a Frobenius group with Frobenius kernel N . Show that each coset of N in G other than N itself is contained in a single conjugacy class of G .

6A.5. Let G be a nonabelian solvable group in which the centralizer of every nonidentity element is abelian. Show that G is a Frobenius group, where $F(G)$ is the Frobenius kernel.

6A.6. Let $A > 1$ and $B > 1$ satisfy the hypothesis of Lemma 6.5 in G . Show that $A \cap B^g > 1$ for some element $g \in G$.

Hint. Consider X and Y corresponding to A and B as in Lemma 6.5.

Note. Since we have not proved Frobenius' theorem that the set appearing in Lemma 6.5 is actually a subgroup, you should not appeal to that fact in these problems.

6A.7. Let A satisfy the hypotheses of Lemma 6.5 in G , and assume $A \subseteq H \subseteq G$.

(a) Given $g \in G$, show that if $A^g \cap H > 1$, then $g \in H$.

(b) If $H \triangleleft G$, show that $H = G$.

Hint. For (a), check that $A^g \cap H$ satisfies the hypothesis of Lemma 6.5 in H and use the previous problem.

6A.8. Let G , A and X be as in Lemma 6.5. If $M \triangleleft G$, show that either $M \subseteq X$ or $X \subseteq M$.

Hint. If $M \cap A > 1$, use the previous problem to show that $AM = G$.

6A.9. Let G , A and X be as in Lemma 6.5, and suppose that $t \in A$ is an involution.

(a) Show that there are at least $|G : A| - 1$ elements $x \in G - A$ such that $x^t = x^{-1}$.

- (b) Show that t inverts every element of the set X .
- (c) Show that t is the unique involution in A , and in particular, t is central in A .
- (d) Show that every element of X has odd order.
- (e) Suppose that x and y lie in X and that $xy^{-1} \in A$. Show that $x^2 = y^2$ and deduce that $x = y$.
- (f) Show that X is a subgroup.

Hint. Lemma 2.14(b) is relevant for (a).

Note. This problem provides a proof of Frobenius' theorem in the case that the subgroup A has even order.

6A.10. Let G , A and X be as in Lemma 6.5.

- (a) Show for each prime divisor p of $|A|$ that A contains a full Sylow p -subgroup P of G and that A controls G -fusion in P .
- (b) If $A > 1$, show that $G'A = G$ and $G' \cap A = A'$.
- (c) If A is solvable, show that the subset X is a subgroup.

Note. By this problem and the previous one, we know that the conclusion of Frobenius' theorem holds if either $|A|$ is even or A is solvable. By the Feit-Thompson odd-order theorem, one of these possibilities must necessarily occur, and this shows that Frobenius' theorem is a consequence of the odd-order theorem. But since the Feit-Thompson proof uses character theory heavily, this certainly does not yield a character-free proof of Frobenius' theorem.

6A.11. Let $A \subseteq G$. Show that A satisfies the hypothesis of Lemma 6.5 in G if and only if $\mathbf{N}_G(T) \subseteq A$ for every nonidentity subgroup T of A .

6B

In this section we present necessary conditions for a group A to be a Frobenius complement. (Recall that we have defined this to mean that there exists some nonidentity group N and a Frobenius action of A on N .) The key idea is to consider "partitioned" groups. A **partition** of G is a collection Π of nonidentity proper subgroups of G such that $\bigcup \Pi = G$ and $X \cap Y = 1$ for every two distinct members X and Y of Π . For example, if $G = D_{2n}$, the dihedral group of order $2n$ with $n > 1$, then G is partitioned by the set Π consisting of the cyclic subgroup C of order n and the n subgroups of order 2 that are not contained in C .

An elementary abelian p -group G of order p^e with $e > 1$ provides another example of a partitioned group. In this situation, the set Π of all

subgroups of order p in G is a partition. It is clear that every two distinct members of Π intersect trivially, and also, since every nonidentity element of G has order p , each such element lies in some subgroup of order p , and so $\bigcup \Pi = G$, as required. In what follows, the cardinality of a partition will be relevant, and in this case, it is especially easy to compute. Each member of Π contains exactly $p - 1$ nonidentity elements, and since G has a total of $p^e - 1$ nonidentity elements, we see that Π consists of exactly $(p^e - 1)/(p - 1)$ subgroups. In particular, if $e = 2$, then $|\Pi| = p + 1$.

We mention one more family of examples. If G is a Frobenius group with kernel N and complement A , let Π be the collection of subgroups consisting of N and all conjugates of A . Since $N \cap A = 1$, it is clear that N intersects trivially with every conjugate of A . Also, every two distinct conjugates of A intersect trivially because A (and each of its conjugates) satisfies statement (2) of Theorem 6.4. Furthermore, by Corollary 6.6, we know that every element of G not in N lies in some conjugate of A , and thus $\bigcup \Pi = G$. In this situation, $A = \mathbf{N}_G(A)$, and so the number of conjugates of A in G is $|G : A| = |N|$, and it follows that $|\Pi| = 1 + |N|$.

6.8. Lemma. *Let Π be a partition of a finite group A , and suppose that A acts via automorphisms on an abelian group U . If U has an element with order not dividing $|\Pi| - 1$, then there exists a member $X \in \Pi$ such that $\mathbf{C}_U(X) > 1$.*

Proof. For each subgroup $H \subseteq A$ and each element $u \in U$, write

$$u_H = \prod_{h \in H} u^h,$$

and observe that this element of U is unambiguously defined since the order of the factors in the product is irrelevant because U is abelian. Also, since the action by an element $h \in H$ simply permutes the factors of u_H , it follows that $(u_H)^h = u_H$ for all $h \in H$, and thus $u_H \in \mathbf{C}_U(H)$. Since we can assume that $\mathbf{C}_U(X) = 1$ for each member $X \in \Pi$, we have $u_X = 1$ for all $u \in U$ and all $X \in \Pi$.

Now fix $u \in U$, and compute that

$$1 = \prod_{X \in \Pi} u_X = u_A u^{|\Pi|-1},$$

where the second equality follows because as a runs over all of the elements of all of the subgroups $X \in \Pi$, each nonidentity element of A occurs exactly once, while the identity of A occurs a total of $|\Pi|$ times. If we choose $u \in U$ such that $u^{|\Pi|-1} \neq 1$, it follows that $u_A \neq 1$, and since $u_A \in \mathbf{C}_U(A) \subseteq \mathbf{C}_U(X)$ for all $X \in \Pi$, the proof is complete. ■

6.9. Theorem. *Let A be a Frobenius complement. Then no subgroup of A is an elementary abelian p -group of order exceeding p , and no solvable subgroup of A is a Frobenius group. Also, every subgroup of A having order pq , where p and q are (possibly equal) primes is cyclic.*

Proof. Let A act on N , where the action is Frobenius and $N > 1$. Suppose that A has a subgroup that is either an elementary abelian p -group of order $p^e > p$ or is a solvable Frobenius group. Since the action of every subgroup of A on N is Frobenius, we can replace A by the appropriate subgroup and assume that A itself is either elementary abelian of order p^e or is solvable and Frobenius. Also, in the elementary abelian case, we can replace A by a subgroup if necessary, and so we can assume that $e = 2$.

In either case, A is solvable and acts coprimely on N , and so if we choose any prime divisor r of $|N|$, Theorem 3.23 guarantees the existence of an A -invariant Sylow r -subgroup R of N . Then $R > 1$, and so $\mathbf{Z}(R) > 1$, and since $\mathbf{Z}(R)$ is characteristic in R , this subgroup is A -invariant. Since the action of A on $\mathbf{Z}(R)$ is Frobenius, we can replace N by $\mathbf{Z}(R)$, and hence we can assume that N is abelian.

Since A is either elementary abelian of order p^2 or is a Frobenius group, A has a partition Π of cardinality $1 + n$, where n is a divisor of $|A|$. (If A is elementary of order p^2 , then $n = p$, and if A is Frobenius, then n is the order of its Frobenius kernel.) Since n divides $|A|$, it is coprime to $|N|$, and thus since N is nontrivial, some element $u \in N$ satisfies $u^n \neq 1$. (In fact, we can take u to be any nonidentity element of N .) It follows by Lemma 6.8 that $\mathbf{C}_N(X) > 1$ for some member $X \in \Pi$. But since $|X| > 1$, this contradicts the fact that the action of A on N is Frobenius, and we conclude that as claimed, the original group A cannot contain an elementary abelian p -group of order exceeding p or a solvable Frobenius group.

What remains is to show that if $B \subseteq A$, where $|B| = pq$, and p and q are possibly equal primes, then B is cyclic. First, if $p = q$, then $|B| = p^2$, and since we have shown that B cannot be elementary abelian, the only other possibility is that it is cyclic, as required. Finally, assume that $p > q$. Then B must have a normal Sylow p -subgroup P of order p . If $Q \in \text{Syl}_q(B)$ and Q acts (by conjugation) nontrivially on P , we have seen that the action of Q on P must be Frobenius. Thus B is a solvable Frobenius group, which we know is impossible. It follows that Q centralizes P , and it is easy to see in this case that $B = PQ$ is cyclic. This completes the proof. ■

6.10. Corollary. *Let $P \in \text{Syl}_p(A)$, where A is a Frobenius complement. Then P contains at most one subgroup of order p .*

Proof. We can assume that $P > 1$. Then $\mathbf{Z}(P) > 1$, and we can choose $Z \subseteq \mathbf{Z}(P)$ with $|Z| = p$. We argue that Z is the only subgroup of order p

in P . Otherwise, let $U \subseteq P$ be a second subgroup of order p , and observe that ZU is a subgroup of order p^2 since $Z \triangleleft P$. Also, ZU is not cyclic since it contains two subgroups of order p , and this contradicts Theorem 6.9. ■

We digress now to classify the p -groups that have at most one subgroup of order p , as in Corollary 6.10. Some obvious examples are the cyclic p -groups, and if $p = 2$, also the generalized quaternion 2-groups. These, we recall, are the 2-groups P of order at least 8 that have a cyclic subgroup $C = \langle c \rangle$ of index 2 and an element a of order 4 in $P - C$ such that $c^a = c^{-1}$. It is not hard to see that if P is generalized quaternion and C is cyclic of index 2 as above, then every element of $P - C$ has order 4. The subgroup of order 2 in C , therefore, is the unique subgroup of order 2 in P .

In fact, cyclic p -groups and generalized quaternion 2-groups are the only p -groups that have just one subgroup of order p .

6.11. Theorem. *Let P be a p -group containing at most one subgroup of order p . Then either P is cyclic, or else $p = 2$ and P is generalized quaternion.*

With only a little extra work, we can prove a stronger theorem, and so although the next result is not directly relevant to Frobenius actions, it seems reasonable to present it here. We shall see that Theorem 6.11 is an immediate consequence.

It is easy to see that an *abelian* p -group with at most one subgroup of order p must be cyclic. (This is immediate from the fundamental theorem of abelian groups.) It follows that if P is any p -group that has at most one subgroup of order p , then all abelian subgroups of P are cyclic. In fact, if $p \neq 2$, the apparently much weaker assumption that all *normal* abelian subgroups of P are cyclic is sufficient to guarantee that P is cyclic. For $p = 2$, however, there are some possibilities other than cyclic and generalized quaternion groups.

6.12. Theorem. *Let P be a p -group in which every normal abelian subgroup is cyclic. Then either P is cyclic, or else $p = 2$ and P is dihedral, generalized quaternion or semidihedral.*

Recall that a 2-group P is dihedral if it has a cyclic subgroup $C = \langle c \rangle$ of index 2 and an involution $a \in P - C$ such that $c^a = c^{-1}$. Like dihedral and generalized quaternion 2-groups, a semidihedral 2-group also has a cyclic subgroup of index 2. Specifically, a 2-group P of order at least 16 is semidihedral if it has a cyclic subgroup $C = \langle c \rangle$ of index 2, and there is an involution a in $P - C$ such that $c^a = zc^{-1}$, where z is the unique element of order 2 in C . (Note that we need to assume that $|P| \geq 16$ because if $|P| = 8$, then c has order 4, and so $zc^{-1} = c$. In that case, a would centralize C and P

would be abelian.) It is not hard to see that most dihedral 2-groups, as well as all generalized quaternion and semidihedral 2-groups actually do satisfy the hypotheses of Theorem 6.12. (The exception among dihedral groups is D_8 , of order 8, which has two noncyclic normal abelian subgroups of order 4.)

In a dihedral or semidihedral group, there is by definition at least one involution outside of the cyclic subgroup of index 2. These groups, therefore, have more than one subgroup of order 2, and so they do not satisfy the hypothesis of Theorem 6.11. It follows that Theorem 6.11 is a consequence of Theorem 6.12.

We begin work toward a proof of Theorem 6.12 with the following.

6.13. Lemma. *Let P be a nonabelian 2-group having a cyclic subgroup $C = \langle c \rangle$ of index 2, and let $a \in P - C$. If $c^a = c^{-1}$, then P is dihedral or generalized quaternion, and if $c^a = zc^{-1}$, where z is the unique involution in C , then P is semidihedral.*

Proof. Since P is nonabelian and $P = \langle a, c \rangle$, the elements a and c cannot commute. In the case where $c^a = c^{-1}$, it follows that the order $o(c) \geq 4$ and in the case where $c^a = zc^{-1}$, we have $o(c) \geq 8$. Now if $c^a = c^{-1}$, then a inverts every element of C , and if $c^a = zc^{-1}$, then $(c^2)^a = (c^2)^{-1}$, and so a inverts every nongenerating element of C . In both cases, therefore, every element of order 4 in C is inverted by a . Since $a^2 \in C$ is centralized by a , the group $\langle a^2 \rangle$ can contain no element of order 4, and thus either $o(a) = 2$ or $a^2 = z$ and $o(a) = 4$. If $c^a = c^{-1}$, therefore, P is either dihedral or generalized quaternion, respectively, and if $c^a = zc^{-1}$ and $o(a) = 2$, then P is semidihedral. In the remaining case, $a^2 = z$ and $c^a = zc^{-1}$, and thus $(ca)^2 = caca = ca^2c^a = 1$. Then $o(ca) = 2$ and since $c^{(ca)} = c^a$, we can replace a by ca to see that P is semidihedral. ■

An easy consequence is the following description of the nonabelian groups of order 8, which we will need in what follows.

6.14. Corollary. *Let P be a nonabelian group of order 8. Then P is isomorphic either to the dihedral group D_8 or to the quaternion group Q_8 .*

Proof. Since P is nonabelian, not every nonidentity element is an involution. We can thus choose $c \in P$ of order 4, and we write $C = \langle c \rangle$, so that C has index 2 in P . If $a \in P - C$ then since P is nonabelian, a cannot centralize c , and so a induces a nontrivial automorphism of C . The cyclic group C of order 4, however, has only one nontrivial automorphism, and we deduce that $c^a = c^{-1}$. The assertion now follows by Lemma 6.13. ■

6.15. Lemma. *Let T be a p -group with order different from 8, and suppose that $|T : \mathbf{Z}(T)| = p^2$. Let C be a cyclic subgroup such that $\mathbf{Z}(T) < C < T$. Then T has a characteristic elementary abelian subgroup of order p^2 .*

Proof. Since $C \triangleleft T$ is abelian and T/C is cyclic, we can apply Lemma 4.6 to conclude that $|C| = |T'| |\mathbf{Z}(T)|$. It follows that $|T'| = p$, and thus $T' \subseteq \mathbf{Z}(T)$, and T has nilpotence class 2.

First, suppose that $p \neq 2$. By Theorem 4.8, the map $\theta : T \rightarrow T$ defined by $\theta(x) = x^p$ is a homomorphism, and we let $K = \ker(\theta)$. Then $K = \{x \in T \mid x^p = 1\}$ is a characteristic subgroup of T , and it suffices to show that $|K| = p^2$. Since $T/\mathbf{Z}(T)$ cannot be cyclic since T is nonabelian, this factor group of order p^2 must be elementary abelian. Thus $\theta(T) \subseteq \mathbf{Z}(T)$, and it follows that $|K| = |T|/|\theta(T)| \geq |T|/|\mathbf{Z}(T)| = p^2$. Finally, $|K : K \cap C| \leq |T : C| = p$, and since $K \cap C$ is a cyclic subgroup of K , we have $|K \cap C| \leq p$. It follows that $|K| \leq p^2$, and we are done in this case.

We can now assume that $p = 2$. In what follows, we will twice use the easy observation that if A is a noncyclic abelian 2-group that has a cyclic subgroup of index 2, then $\{a \in A \mid a^2 = 1\}$ is a characteristic elementary abelian subgroup of order 4. First, applying this to the group T/T' (which is not cyclic because T' is central and T is not abelian) we obtain a characteristic elementary abelian subgroup E/T' of order 4, and thus E is characteristic in T and $|E| = 8$.

Now E is noncyclic, and hence $E \neq C$. Also, $E \neq T$ since $|T| \neq 8$, and we conclude that $E \not\subseteq C$. It follows that $E \cap C$ is a proper subgroup of C , which, therefore, is contained in $\mathbf{Z}(T)$. Also, $E \cap C$ is a cyclic subgroup of E with index 2, and hence E is abelian but not cyclic. It follows that E has a characteristic elementary abelian subgroup K of order 4, and since E is characteristic in T , so too is K . This completes the proof. ■

Next, we present an elementary number-theoretic fact.

6.16. Lemma. *Let p be prime, and let e be a positive integer. Suppose that i is an integer such that $i^p \equiv 1 \pmod{p^e}$. Then one of the following occurs.*

- (a) $i \equiv 1 \pmod{p^{e-1}}$.
- (b) $p = 2$ and $i \equiv -1 \pmod{2^e}$.
- (c) $p = 2$ and $i \equiv 2^{e-1} - 1 \pmod{2^e}$.

Proof. First, suppose that $p > 2$. If $i = 1$, then (a) certainly holds, and so we can assume that $i \neq 1$, and we write $i - 1 = mp^t$ where p does not divide m and $t \geq 0$. We have $i \equiv i^p \equiv 1 \pmod{p}$, where the first congruence follows

by Fermat's little theorem, and thus $t > 0$. Also,

$$i^p = (1 + mp^t)^p \equiv 1 + mp^{t+1} + \binom{p}{2} m^2 p^{2t} \pmod{p^{3t}}.$$

Since p is odd, the binomial coefficient $\binom{p}{2}$ is divisible by p , and we have $i^p \equiv 1 + mp^{t+1} \pmod{p^{2t+1}}$. It follows that the highest power of p dividing $i^p - 1$ is p^{t+1} . By hypothesis, however, p^e divides $i^p - 1$, and thus $e \leq t + 1$. Then $e - 1 \leq t$, and we have $i \equiv 1 \pmod{p^{e-1}}$, as required.

Now assume $p = 2$, so that 2^e divides $i^2 - 1 = (i - 1)(i + 1)$. Since one of the factors $i - 1$ or $i + 1$ is not divisible by 4, the other must be divisible by 2^{e-1} , and thus $i \equiv \pm 1 \pmod{2^{e-1}}$. Assuming that (a) fails, we have $i \equiv -1 \pmod{2^{e-1}}$, and we can write $i = -1 + a2^{e-1}$ for some integer a . If a is even, then $i \equiv -1 \pmod{2^e}$ and (b) holds. Otherwise, $a = 2b + 1$ for some integer b , and so $i = -1 + (2b + 1)2^{e-1} \equiv 2^{e-1} - 1 \pmod{2^e}$, proving (c). ■

We can now assemble the pieces.

Proof of Theorem 6.12. Let C be maximal among abelian normal subgroups of P . By hypothesis, C is cyclic, so we can assume that $C < P$. Also, $C = \mathbf{C}_P(C)$ since otherwise, we could find a subgroup $B \triangleleft P$ with $C \subseteq B \subseteq \mathbf{C}_P(C)$, where $|B : C| = p$. Since C is central in B and B/C is cyclic, it would follow that B is abelian, which contradicts the choice of C . Thus $P/C = P/\mathbf{C}_P(C)$ is isomorphically embedded in $\text{Aut}(C)$, which is abelian, and thus P/C is abelian. Also, if $|C| = 4$, it follows that $|P/C| = 2$ and $|P| = 8$, and by Corollary 6.14, there is nothing to prove in this case. We can assume, therefore, that $|C| \neq 4$, and we write $|C| = p^e$.

Let $T/C \subseteq P/C$ have order p , and observe that $T \triangleleft P$ since P/C is abelian. Also, T is not abelian and $|T| \neq 8$ since $|C| \neq 4$. Since T cannot have a characteristic elementary abelian subgroup of order p^2 , it follows by Lemma 6.15 that c^p cannot be central in T , where $C = \langle c \rangle$. Thus $(c^p)^a \neq c^p$, where we have chosen $a \in T - C$.

We can write $c^a = c^i$ for some integer i . Since $a^p \in C$, it follows that

$$c = c^{a^p} = c^{i^p},$$

and since c has order p^e , we conclude that $i^p \equiv 1 \pmod{p^e}$. Furthermore, $c^p \neq (c^p)^a = (c^p)^i$, and since c^p has order p^{e-1} , we conclude that $i \not\equiv 1 \pmod{p^{e-1}}$. It follows by Lemma 6.16 that $p = 2$ and $i \equiv -1 \pmod{2^{e-1}}$. Thus $(c^2)^a = (c^2)^{-1}$.

Now P/C acts faithfully on C , and by the computation of the previous paragraph, every involution in the abelian group P/C acts to invert the element c^2 , which has order at least 4. It follows that there is only one such involution because if there were two, their product would be an involution

that centralizes and does not invert c^2 . Since P/C is an abelian 2-group with just one involution, we conclude that P/C is cyclic.

We argue next that $|P/C| = 2$. Otherwise, the element a is a square modulo C , and it follows that $i \equiv j^2 \pmod{2^e}$ for some integer j . But $i \equiv -1 \pmod{2^{e-1}}$, and since $e \geq 3$, it follows that $j^2 \equiv -1 \pmod{4}$, and this is not possible.

Now $P = T$, and by Lemma 6.16, either $i \equiv -1 \pmod{2^e}$ or $i \equiv 2^{e-1} - 1 \pmod{2^e}$. In other words, either $c^a = c^{-1}$ or $c^a = zc^{-1}$, where $z = c^{2^{e-1}}$ is the involution in C . The result now follows by Lemma 6.13. ■

We return now to the study of Frobenius complements.

6.17. Corollary. *Suppose that A is a Frobenius complement. Then each Sylow subgroup of A is cyclic or generalized quaternion.*

Proof. By Corollary 6.10, a Sylow p -subgroup of A has at most one subgroup of order p . By Theorem 6.11, such a group must be cyclic or generalized quaternion. ■

Observe that by Corollary 6.17, all Sylow subgroups of an abelian Frobenius complement A are cyclic, and so A itself must be cyclic.

6.18. Corollary. *Let A be a Frobenius complement of odd order. Then A' and A/A' are cyclic and have coprime orders.*

Proof. By Corollary 6.17, all Sylow subgroups of A are cyclic. The result now follows by Theorem 5.16. ■

We know more about the structure of a Frobenius complement than what its Sylow subgroups look like, and we can use this to derive more subtle information. For example, we have the following.

6.19. Theorem. *Let A be a Frobenius complement of odd order. Then A has a unique subgroup of order p for each prime p dividing $|A|$.*

Proof. First, consider a prime divisor r of $|A'|$. Then r does not divide $|A/A'|$ by Corollary 6.18, and thus every subgroup R of order r in A actually lies in A' . Since A' is cyclic, however, it has only one subgroup of order r , and thus R is unique, and in particular, $R < A$.

Now let q be a prime divisor of $|A|$ such that q does not divide $|A'|$. Then q divides the order of the cyclic group A/A' , and so A/A' has a unique subgroup X/A' of order q . Then every subgroup $Q \subseteq A$ of order q lies in X , and in fact $X = A'Q$. Also, $Q \in \text{Syl}_q(X)$ since q does not divide $|A'|$. To prove that Q is unique, therefore, it suffices to show that $Q < X$.

Let $R \subseteq A'$ be an arbitrary subgroup of prime order, say r . We know that $R \triangleleft A$, and thus RQ is a subgroup of A of order rq . It follows that RQ is cyclic by Theorem 6.9, and in particular, Q centralizes R . Thus $\mathbf{C}_{A'}(Q)$ contains every subgroup of A' having prime order.

Since A' is abelian and has order coprime to q , it follows by Fitting's theorem that $A' = [A', Q] \times \mathbf{C}_{A'}(Q)$. Since the second factor contains every prime order subgroup of A' , the first factor can contain no such subgroup, and we conclude that $[A', Q] = 1$. Thus Q centralizes A' , and so $Q \triangleleft A'Q = X$, as required. ■

Next, we present two results that are needed in Chapter 7.

6.20. Lemma. *Suppose that A is a finite abelian group that acts faithfully on a finite group N , where $|A|$ and $|N|$ are coprime. Assume in addition that the action of A on every proper A -invariant subgroup of N is trivial. Then A is cyclic.*

We will deduce this as a corollary of the following.

6.21. Theorem. *Suppose that A is a finite abelian group and that it acts on a finite group N , where $|A|$ and $|N|$ are coprime. If A is not cyclic, then*

$$N = \langle \mathbf{C}_N(a) \mid 1 \neq a \in A \rangle.$$

Proof. The assertion is trivial if $N = 1$, so we assume that $N > 1$, and we proceed by induction on $|N|$. Write

$$K = \langle \mathbf{C}_N(a) \mid 1 \neq a \in A \rangle,$$

so that our goal is to show that $K = N$.

If M is a proper subgroup of N that admits the action of A , then by the inductive hypothesis,

$$M = \langle \mathbf{C}_M(a) \mid 1 \neq a \in A \rangle \subseteq K,$$

and so K contains every proper A -invariant subgroup of N . Now assume that $K < N$, and choose a prime divisor p of $|N : K|$. Since A is certainly solvable, and its order is coprime to $|N|$, we know that there exists some A -invariant Sylow p -subgroup P of N , and we see that $P \not\subseteq K$ since p divides $|N : K|$. It follows that $P = N$, and so N is a p -group, and thus N' is a proper A -invariant subgroup. Then $N' \subseteq K$, and it follows that $K \triangleleft N$. Also, K is A -invariant since it is uniquely determined by A and N .

Now consider the induced action of A on $\overline{N} = N/K$. Since “fixed points come from fixed points” in coprime actions, it follows that $\mathbf{C}_{\overline{N}}(a) = \overline{\mathbf{C}_N(a)}$ for all elements $a \in A$. But if $1 \neq a \in A$, then $\mathbf{C}_N(a) \subseteq K$, and so $\overline{\mathbf{C}_N(a)}$ is trivial. It follows that $\mathbf{C}_{\overline{N}}(a)$ is trivial, and thus the action of A on the

nontrivial group \overline{N} is Frobenius. But A is not a Frobenius complement since it is abelian but not cyclic. This contradiction completes the proof. ■

Proof of Lemma 6.20. Since A is abelian, the subgroup $C_N(a)$ is A -invariant for all $a \in A$. (This is because $C_N(a)$ is uniquely determined by the element a , which is invariant under conjugation by A .) Also, if $a \neq 1$, then $C_N(a) < N$ because the action of A on N is faithful, and thus by hypothesis, $C_N(a) \subseteq C_N(A)$ for all nonidentity elements $a \in A$. If A is not cyclic, however, then by Theorem 6.21, the subgroups $C_N(a)$ generate N , and thus $N = C_N(A)$. Since A acts faithfully, this yields $A = 1$, and this is a contradiction, since we assumed that A is not cyclic. The result now follows. ■

Problems 6B

6B.1. Show that every Frobenius group contains a solvable Frobenius subgroup, and deduce that a Frobenius complement cannot have a Frobenius group as a subgroup.

6B.2. Let A act faithfully on N , where A is abelian, and assume that no nonidentity proper subgroup of N is A invariant. Show that A is cyclic.

Hint. Let p be a prime divisor of $|N|$ and let $P \in \text{Syl}_p(A)$. Then $C_N(P)$ is A -invariant and nontrivial.

6B.3. Show that if the coprimeness assumption in Theorem 6.21 is dropped, the result becomes false.

6B.4. Suppose that G has a partition Π such that $[X, Y] = 1$ for every two distinct members X and Y of Π .

(a) Show that G is abelian.

(b) Show that the elements of G have equal prime orders, so that G is elementary abelian.

Hint. For (b), consider $x \in X \in \Pi$ and $y \in Y \in \Pi$, where $X \neq Y$. If $o(x) < o(y)$, consider the element $(xy)^{o(x)}$. In which member of Π does it lie?

Note. The hypotheses of the previous problem are automatically satisfied if the members of Π are all normal in G .

6B.5. Suppose that G has a partition consisting of subnormal subgroups. Show that G is nilpotent.

Hint. Working by induction on $|G|$, show that every subgroup $H < G$ that is not contained in some member of the partition is nilpotent. Deduce that every member of the partition that is not contained in $F(G)$ is normal in G and has prime index.

6B.6. Let C be a cyclic 2-group of order at least 8. Show that C has exactly three automorphisms of order 2.

6B.7. Let P be a nonabelian 2-group that has a cyclic subgroup of index 2. If $|P : \mathbf{Z}(P)| > 4$, show that P is dihedral, semidihedral or generalized quaternion.

6B.8. Let P be a 2-group of order at least 8, and assume that $|P : P'| = 4$. Show that P is dihedral, semidihedral or generalized quaternion.

Hint. Let $Z \subseteq G' \cap \mathbf{Z}(G)$ have order 2. Working by induction on $|P|$, deduce that P has an abelian subgroup A of index 2 and that A is either cyclic or is the direct product of Z with a cyclic group. In the latter case, and assuming that $|P| \geq 16$, deduce that $Z < \mathbf{Z}(P)$ and derive a contradiction.

Note. This problem proves a theorem of O. Taussky-Todd.

6B.9. Let G be solvable, and assume that every element of G has prime-power order. Show that $|G|$ is divisible by at most two primes.

6C

We now begin work toward a proof of the theorem of Thompson's Ph.D. thesis: Frobenius kernels are nilpotent. We prove this first under the additional assumption that the given Frobenius kernel is solvable. (This special case, which is needed for Thompson's result, appears in a 1957 paper of G. Higman, where it is described as being already known.)

6.22. Theorem. *Let N be a solvable Frobenius kernel. Then N is nilpotent.*

Proof. By hypothesis, there exists a nontrivial group A having a Frobenius action on N . Since the action of every subgroup of A on N is also Frobenius, we can replace A by a subgroup of prime order, and so we can assume that $|A| = p$, a prime. Let $G = N \rtimes A$, and as usual, view N and A as subgroups of G , where $N \triangleleft G$ is complemented by A .

Assuming that N is not nilpotent, we proceed by induction on $|N|$. Since $N > 1$, we can choose a minimal normal subgroup U of G , with $U \subseteq N$. The induced action of A on N/U is Frobenius by Theorem 6.2, and of course

N/U is solvable. By the inductive hypothesis, therefore, N/U is nilpotent, and thus $N^\infty \subseteq U$. But $N^\infty > 1$ since N is not nilpotent, and of course, $N^\infty \triangleleft G$. The minimality of U , therefore, yields $U = N^\infty$, and thus U is the unique minimal normal subgroup of G contained in N . (Any other one would also have to be N^∞ .)

Since U is solvable and is minimal normal in G , Lemma 3.11 guarantees that U must be an abelian q -group for some prime q . But N is not a q -group since it is not nilpotent, and so we can choose a prime divisor $r \neq q$ of $|N|$. Let $R \in \text{Syl}_r(N)$, and choose R to be A -invariant. (Although the existence of an A -invariant Sylow r -subgroup follows via Theorem 3.23, we do not really need the full strength of that theorem here. This is because $|A| = p$ and $|\text{Syl}_r(N)|$ is not divisible by p , and so a simple counting argument suffices to find an A -invariant Sylow r -subgroup of N .) Observe that R is not normal in N since, otherwise, it would be characteristic, and hence normal in G . But $R \not\subseteq U$, and so this would contradict the fact that U is the unique minimal normal subgroup of G contained in N .

Now RU/U is a Sylow r -subgroup of the nilpotent group N/U , and thus $RU/U \triangleleft N/U$ and $RU \triangleleft N$. Also, RU admits the action of A , and so RU is a solvable Frobenius kernel. If $RU < N$, then RU is nilpotent by the inductive hypothesis, and hence R is characteristic in RU , and hence $R \triangleleft N$, which is a contradiction. We deduce that $RU = N$.

Since AR is a Frobenius group, it has a partition Π consisting of R and the $|R|$ conjugates of A in AR . Then $|\Pi| - 1 = |R|$ is a power of r , and so this number is coprime to $|U|$. By Lemma 6.8, therefore, some member $X \in \Pi$ has nontrivial fixed points in the abelian group U . The action of every G -conjugate of A on U is Frobenius, however, and so X cannot be one of the conjugates of A . We deduce that $X = R$, and thus since U is abelian and $RU = N$, we have

$$1 < C_U(R) \subseteq Z(RU) = Z(N).$$

Since U is the unique minimal normal subgroup of G contained in N and $Z(N)$ is nontrivial and normal in G , we conclude that $U \subseteq Z(N)$, and thus $R \triangleleft UR = N$. This is a contradiction, and the proof is complete. ■

Next, we state a result of Thompson that will enable us to prove the theorem of his thesis, which was that all Frobenius kernels are nilpotent (and not just solvable Frobenius kernels, as in Theorem 6.22). Actually, the main result of Thompson's thesis was a criterion for a group to have a normal p -complement, where p is an odd prime; the result about Frobenius kernels is a comparatively easy corollary. About five years after he completed his degree, Thompson found a much better version of his normal p -complement theorem with a very much easier proof, and that is the result we present and

prove in Chapter 7. Here we give only a partial statement of this improved theorem.

6.23. Theorem (Thompson). *Let $P \in \text{Syl}_p(G)$, where G is a finite group and $p \neq 2$, and assume that $\mathbf{N}_G(X)$ has a normal p -complement for every nonidentity characteristic subgroup X of P . Then G has a normal p -complement.*

First, observe that this can be viewed as a strong form of Frobenius' normal p -complement theorem, which is our Theorem 5.26. Recall that Frobenius' theorem tells us that to prove that G has a normal p -complement, it suffices to show that $\mathbf{N}_G(X)$ has a normal p -complement for every nonidentity p -subgroup X of G . It is a triviality (by Sylow theory) that in Frobenius' theorem, it is enough to consider only p -subgroups X that are contained in some fixed Sylow p -subgroup P of G . The force of Theorem 6.23 is that for $p \neq 2$, it suffices to restrict attention to nonidentity *characteristic* subgroups X of P ; it is not necessary to consider all nonidentity subgroups of P . (The normal p -complement theorem of Thompson's thesis can also be viewed as a strong form of Frobenius' theorem, valid for $p \neq 2$. It is somewhat more complicated to state, however.)

We mention that the condition $p \neq 2$ in Theorem 6.23 is essential. Consider, for example, $G = S_4$, the symmetric group of order 24. A Sylow 2-subgroup P of G is isomorphic to the dihedral group D_8 , and the nonidentity characteristic subgroups of P are P , the unique cyclic subgroup of order 4 in P and $\mathbf{Z}(P)$, of order 2. It is easy to check that the normalizer in G of each of these subgroups is P itself, and so these normalizers all have normal 2-complements. The group G , however, does not have a normal 2-complement.

As we shall see in Chapter 7, it is not actually necessary to consider *all* nonidentity characteristic subgroups X of P ; two of them suffice. One of these is the center $\mathbf{Z}(P)$, and the other is the Thompson subgroup $\mathbf{J}(P)$, which we will define. Of course, if $P > 1$, then $\mathbf{Z}(P) > 1$, and as we shall see, also $\mathbf{J}(P) > 1$.

Assuming Theorem 6.23, we now present the main result of this section.

6.24. Theorem. *Let N be a Frobenius kernel. Then N is nilpotent.*

Proof. As in the proof of Theorem 6.22, there exists a group A of prime order p such that A has a Frobenius action on N . Proceeding by induction on $|N|$, suppose first that there exists a normal A -invariant subgroup M of N with $1 < M < N$. Then the action of A on M is Frobenius, and by Corollary 6.2, so too is the action of A on N/M . By the inductive hypothesis, therefore, both M and N/M are nilpotent, and thus N is solvable. It follows

by Theorem 6.22 that N is nilpotent, and we are done in this case. We can assume, therefore, that N contains no nontrivial proper A -invariant normal subgroup.

We argue now that N is an r -group for some prime r , and thus N is nilpotent, as wanted. Otherwise, $|N|$ has at least two prime divisors, and so we can choose an odd prime r dividing $|N|$. Let R be an A -invariant Sylow r -subgroup of N . (As in the proof of Theorem 6.22, the existence of an A -invariant Sylow r -subgroup follows by a simple counting argument because $|A|$ is prime.)

Let X be a nonidentity characteristic subgroup of R . Since R is A -invariant, it follows that X is also A -invariant. Furthermore, $X < N$ because N is not an r -group, and so by the result of the previous paragraph, X cannot be normal in N . Then $\mathbf{N}_N(X)$ is a proper A -invariant subgroup of N , and so by the inductive hypothesis, $\mathbf{N}_N(X)$ is nilpotent, and hence it has a normal r -complement. (Every nilpotent group has a normal r -complement.) It follows by Theorem 6.23 that N has a normal r -complement K , and we have $1 < K < N$ since N is not an r -group, but it does have order divisible by r . Also, K is characteristic in N , and so it is A -invariant. This contradicts the result of the first paragraph, and so the proof is complete. ■

Problems 6C

6C.1. Let $\sigma \in \text{Aut}(G)$, and suppose that σ fixes only the identity in G .

- (a) If σ has prime order, show that G is nilpotent.
- (b) Show by example that G need not be nilpotent if σ has order 4.

Hint. There exists an example for (b) with $|G| = 75$.

6C.2. Let A be elementary abelian of order p^2 , and suppose that A acts on a nonnilpotent group N via automorphisms. Assume that $\mathbf{C}_N(A) = 1$.

- (a) Show that N has nilpotent subgroups $K_i > 1$ for $1 \leq i \leq p+1$ such that $K_i \cap K_j = 1$ when $i \neq j$.
- (b) Now fix a prime q , and let Q_i be the unique Sylow q -subgroup of K_i , where the K_i are the subgroups of (a). Let $X = \langle Q_i \mid 1 \leq i \leq p+1 \rangle$. Show that $X \in \text{Syl}_q(N)$.

Hint. For (b), consider an A -invariant Sylow q -subgroup Q of N . Show first that $X \subseteq Q$. If $X < Q$, show that $X \subseteq Y \triangleleft Q$, for some A -invariant subgroup Y that is proper in Q . Show that the action of A on Q/Y is Frobenius.

The Thompson Subgroup

7A

In this chapter, we complete the proof of Thompson's theorem that Frobenius kernels are nilpotent. The missing ingredient in our partial proof in Chapter 6 is to show that if $p \neq 2$, then a sufficient condition for a group G to have normal p -complement is that for every nonidentity characteristic subgroup X of some Sylow p -subgroup P of G , the subgroup $\mathbf{N}_G(X)$ has a normal p -complement. (Since every subgroup of a group that has a normal p -complement must also have a normal p -complement, this is clearly a necessary condition too, but, of course, that fact is far less interesting.)

Thompson's first normal p -complement criterion appeared in his 1959 Ph.D. thesis, with a long and subtle proof. Then in 1964, Thompson published a much shorter (though still subtle) proof of a stronger theorem, and that is the theorem and proof we present in this chapter. (Thompson's 1964 paper appeared in the very first issue of the *Journal of Algebra*, which was an auspicious beginning for that periodical.) Thompson showed in his *Journal of Algebra* paper that if $p \neq 2$, then a group G has a normal p -complement provided that $\mathbf{N}_G(X)$ has a normal p -complement for just two specific characteristic subgroups X of P , where $P \in \text{Syl}_p(G)$. These two critical characteristic subgroups are the center $\mathbf{Z}(P)$ and the Thompson subgroup $\mathbf{J}(P)$, both of which are nontrivial if P is nontrivial. (We know, of course, that the center of a nontrivial p -group is nontrivial, and as we shall see when we present the definition, the Thompson subgroup of a nontrivial p -group is also guaranteed to be nontrivial.) Of course, if the normalizers

of *all* nontrivial characteristic subgroups of P have normal p -complements, then in particular, $\mathbf{N}_G(\mathbf{Z}(P))$ and $\mathbf{N}_G(\mathbf{J}(P))$ have normal p -complements, and so Thompson's 1964 theorem yields our Theorem 6.23, which was the key to the proof that Frobenius kernels are nilpotent in Chapter 6. In fact, Thompson's 1964 theorem is slightly stronger than we have just stated since we can replace the normalizer of $\mathbf{Z}(P)$ with the centralizer of $\mathbf{Z}(P)$. (Since $\mathbf{C}_G(\mathbf{Z}(P)) \subseteq \mathbf{N}_G(\mathbf{Z}(P))$, the requirement that the centralizer should have a normal p -complement is weaker than, and is implied by, the corresponding assumption for the normalizer.)

7.1. Theorem (Thompson). *Let $P \in \text{Syl}_p(G)$, where G is a finite group and $p \neq 2$, and assume that $\mathbf{C}_G(\mathbf{Z}(P))$ and $\mathbf{N}_G(\mathbf{J}(P))$ have normal p -complements. Then G has a normal p -complement.*

As we have explained, once we complete the proof of Theorem 7.1, we will have established that all Frobenius kernels are nilpotent. The Thompson subgroup $\mathbf{J}(P)$ has other applications too, and in particular, it provides a crucial ingredient in the group-theoretic proof of Burnside's $p^a q^b$ -theorem that we present later in this chapter. For that reason, we prove somewhat more about the Thompson subgroup than the minimum needed for the proof of Theorem 7.1.

Unfortunately, the literature contains several slightly different definitions of “the” Thompson subgroup of a p -group P , and in general, these definitions yield different subgroups, all of which have been referred to as $\mathbf{J}(P)$. In particular, the version of $\mathbf{J}(P)$ that we are about to define is not always equal to Thompson's $\mathbf{J}(P)$. Our definition is slightly easier to use than that in Thompson's paper, however, and we feel that this justifies the risk of confusion caused by competing definitions.

Given a p -group P , let $\mathcal{E}(P)$ be the set of all of those elementary abelian subgroups of P that have the maximum possible order. Then the **Thompson subgroup** $\mathbf{J}(P)$ of P is the subgroup generated by all of the members of $\mathcal{E}(P)$. For example, if P is the dihedral group of order 8, then obviously, P does not contain an elementary abelian subgroup of order 8. But P does contain an elementary abelian subgroup of order 4, and so $\mathcal{E}(P)$ is the set of all elementary abelian subgroups of order 4 in P . There are two of these, and together they generate the whole group P , and thus $\mathbf{J}(P) = P$ in this case. Of course, if P is nontrivial, then it must contain a nontrivial elementary abelian subgroup, for instance, one of order p , and thus the set $\mathcal{E}(P)$ contains at least one nontrivial subgroup. It follows that $\mathbf{J}(P) > 1$, as we mentioned previously.

In his 1964 paper, Thompson did not restrict attention to elementary abelian subgroups. Instead, he defined $\mathbf{J}(P)$ to be the subgroup generated by

all abelian subgroups of P of largest possible rank. (The **rank** of an abelian p -group A is the integer r such that the unique largest elementary abelian subgroup $\Omega_1(A)$ has order p^r . Equivalently, if the abelian p -group A is decomposed as a direct product of nontrivial cyclic factors, then the rank of A is the number of such factors.) Since an elementary abelian subgroup with maximum possible order in P is an abelian subgroup of maximum possible rank, we see that our subgroup $\mathbf{J}(P)$ is always contained in Thompson's, but it can be properly smaller. (The containment is proper, for example, if P is abelian, but not elementary abelian.) Yet another variation on the definition that has appeared in the literature is to consider the subgroup of P generated by all abelian subgroups of largest possible order.

An immediate consequence of the definition is the following.

7.2. Lemma. *Let $\mathbf{J}(P) \subseteq Q \subseteq P$, where P is a p -group. Then $\mathbf{J}(P) = \mathbf{J}(Q)$, and in particular, $\mathbf{J}(P)$ is characteristic in Q .*

Proof. Since $\langle \mathcal{E}(P) \rangle = \mathbf{J}(P) \subseteq Q$, it follows that every maximal-order elementary abelian subgroup of P is contained in Q , and because $Q \subseteq P$, these are maximal-order elementary abelian subgroups of Q . Every maximal-order elementary abelian subgroup of Q , therefore, has the same order as the members of $\mathcal{E}(P)$, and hence is a member of $\mathcal{E}(P)$. It follows that $\mathcal{E}(Q) = \mathcal{E}(P)$, and thus $\mathbf{J}(Q) = \mathbf{J}(P)$. ■

Before we can begin our proof of Theorem 7.1, we need a number of preliminary results. The first of these is a fairly technical lemma about the general linear group $GL(2, p)$, which, we recall, is the group of invertible 2×2 matrices over the field F of order p .

7.3. Lemma. *Let $G = GL(2, p)$, where $p \neq 2$ is prime, and let $P \subseteq G$ be a p -subgroup. Suppose $P \subseteq \mathbf{N}_G(L)$, for some subgroup L of G , where $|L|$ is not divisible by p , and assume further that a Sylow 2-subgroup of L is abelian. Then $P \subseteq \mathbf{C}_G(L)$.*

The condition that $p \neq 2$ in Lemma 7.3 is necessary since $GL(2, 2)$ is isomorphic to the symmetric group S_3 , and so there is a p' -group L of order 3 normalized but not centralized by a Sylow p -subgroup P of order 2. The somewhat unnatural requirement that L should have an abelian Sylow 2-subgroup also cannot be omitted, at least when $p = 3$. If $G = GL(2, 3)$, then G has a subgroup L of order 8 that is normalized but not centralized by a Sylow 3-subgroup P , which has order 3. (The product LP of order 24 is the special linear group $SL(2, 3)$, which is the set of matrices with determinant 1 in G .) This is not a counterexample to Lemma 7.3, however, since L is a nonabelian 2-group, isomorphic to the quaternion group Q_8 . In fact, it is only for $p = 3$ that such an example can occur, and so Lemma 7.3 could be

strengthened by requiring the condition on a Sylow 2-subgroup of L only if $p = 3$. When we apply the lemma, however, we will know that L is abelian, and so we have no need for a stronger result.

We digress briefly to discuss general linear groups in general, and also special linear groups and certain other related groups. (We saw some of these groups in Chapter 1, and we study them further in Chapter 8.)

If F is an arbitrary field and n is a positive integer, then $GL(n, F)$ is the group of all invertible $n \times n$ matrices over F , and the special linear group $SL(n, F)$ is the subgroup of $GL(n, F)$ consisting of those matrices that have determinant equal to 1. Since the determinant map is a homomorphism from $GL(n, F)$ onto the multiplicative group F^\times of F , it follows that $SL(n, F)$, which is the kernel of this homomorphism, must be a normal subgroup. Also, we have $GL(n, F)/SL(n, F) \cong F^\times$.

Now suppose that F is finite, so that $|F| = q$, where q is a prime power. Since F is the unique field (up to isomorphism) of order q , it is no loss to write $GL(n, q)$ in place of $GL(n, F)$, and in fact, this notation is fairly common. Similarly, we write $SL(n, q)$ for the corresponding special linear group, which is a normal subgroup of index $|F^\times| = q - 1$ in $GL(n, q)$.

We can compute $|GL(n, q)|$ by counting the number of ways we can construct an $n \times n$ matrix with linearly independent rows, where each entry comes from the field F of order q . Of course, there are a total of q^n row vectors of length n over F . Each of these other than the zero row is a possibility for the first row of our matrix, and so there are exactly $q^n - 1$ possible first rows. To keep the rows linearly independent, we must not allow the second row to be one of the q different scalar multiples of the (nonzero) first row, so after the first row is chosen, there are exactly $q^n - q$ possibilities for the second row. After the first two (linearly independent) rows are selected, we must exclude all of their q^2 different linear combinations from appearing as the third row, and this leaves $q^n - q^2$ possibilities for the third row. Continuing like this, we see that there are exactly $q^n - q^{k-1}$ possibilities for the k th row, and we deduce that

$$|GL(n, q)| = \prod_{i=0}^{n-1} (q^n - q^i) = q^N \prod_{j=1}^n (q^j - 1),$$

where $N = 1 + 2 + \cdots + (n-1) = n(n-1)/2$. In particular, $|GL(2, q)| = (q^2 - 1)(q^2 - q) = q(q-1)^2(q+1)$, and $|SL(2, q)| = q(q-1)(q+1)$.

Now consider the subgroup $P \subseteq GL(n, q)$ consisting of the matrices that have zeros below the diagonal, ones on the diagonal and arbitrary elements of F in all above-diagonal positions. (Note that P really is a subgroup, and that $P \subseteq SL(n, q)$.) Since row k of an $n \times n$ matrix contains exactly $k-1$ above-diagonal positions, we see that the total number of above-diagonal

positions in an $n \times n$ matrix is $1 + 2 + \cdots + (n - 1) = N$, where N is as before. Then $|P| = q^N$, and thus $|GL(n, q)| = |P|m$, where m is a product of numbers of the form $q^j - 1$, and so m is relatively prime to q . Since q is a power of some prime, say p , we see that the subgroup P is a Sylow p -subgroup of $GL(n, q)$. Note that if $n > 1$, we can easily find a second Sylow p -subgroup, different from P , by taking lower triangular matrices in place of the upper triangular subgroup P .

The scalar matrices in $GL(n, q)$ are the scalar multiples of the identity matrix, and so there are exactly $q - 1$ of these, and it is easy to see that these matrices form the center $\mathbf{Z}(GL(n, q))$. The factor group $GL(n, q)/\mathbf{Z}(GL(n, q))$ is the projective general linear group, and is denoted $PGL(n, q)$. The scalar matrices that lie in $SL(n, q)$ are the matrices of the form $\alpha \cdot 1$, where $\alpha^n = 1$, and in fact, these form the center $\mathbf{Z}(SL(n, q))$. Writing $Z = \mathbf{Z}(SL(n, q))$, we see that $|Z|$ is equal to the number d of elements $\alpha \in F^\times$ such that $\alpha^n = 1$. Since F^\times is cyclic of order $q - 1$, it follows that $d = (n, q - 1)$, the greatest common divisor. By definition, the projective special linear group $PSL(n, q)$ is the factor group $SL(n, q)/Z$. For $n \geq 2$, this group is simple except when $n = 2$ and q is 2 or 3. (In fact, $PSL(n, F)$ is also simple when $n \geq 2$ and F is an infinite field.)

Taking $n = 2$, we have $|PSL(2, q)| = q(q - 1)(q + 1)/d$, where $d = 1$ if q is a power of 2 and $d = 2$ if q is odd. In particular, for prime powers $q = 4, 5, 7, 8, 9, 11$ we have $|PSL(2, q)| = 60, 60, 168, 504, 360, 660$, respectively, and these account for all of the nonabelian simple groups of order at most 1000. (We have not omitted the alternating groups A_5 and A_6 since $PSL(2, 4) \cong A_5 \cong PSL(2, 5)$ and $PSL(2, 9) \cong A_6$.) We mention also that $PSL(2, 7) \cong PSL(3, 2)$ and $A_8 \cong PSL(4, 2)$. In fact, these are the only isomorphisms among alternating groups and the simple groups of type $PSL(n, q)$. (The simple groups $PSL(3, 4)$ and A_8 have equal orders, but they are not isomorphic.)

Finally, we mention one way that general linear groups arise in abstract group theory. Consider an elementary abelian p -group E of order p^n , and view E as an additive group. Then E can be identified with a vector space of dimension n over the field of order p , and under this identification, we see that $\text{Aut}(E) \cong GL(n, p)$. This observation (in the case $n = 2$) is crucial to the proof of Theorem 7.1, and that is why Lemma 7.3 is relevant.

In order to prove Lemma 7.3, we need the following observation about the groups $SL(2, q)$, where q is odd.

7.4. Lemma. *If q is odd, then the negative of the identity matrix is the unique involution in $SL(2, q)$.*

This can be proved by a computational argument along the following lines. If t is an involution in $SL(2, q)$, then the fact that $t^2 = 1$ yields four nonlinear equations that must be satisfied by the four entries of the matrix t , and the fact that $\det(t) = 1$ yields one more equation. It is not hard to show that if the characteristic is different from 2, these five equations have just two solutions, corresponding to $t = I$ and $t = -I$, where I is the 2×2 identity matrix. We prefer the following more conceptual proof, however.

Proof of Lemma 7.4. Let $t \in SL(2, q)$ be an involution other than $-I$. Write $f(X)$ to denote the polynomial $X^2 - 1$, and observe that $f(t) = 0$. Since neither the polynomial $X - 1$ nor the polynomial $X + 1$ yields 0 when t is substituted for X , it follows that $f(X) = X^2 - 1$ is the minimal polynomial for t . The Cayley-Hamilton theorem asserts that the minimal polynomial of an arbitrary square matrix divides the characteristic polynomial, and in our situation, where t is a 2×2 matrix, we know that the characteristic polynomial of t has degree 2, and hence $f(X)$ is the characteristic polynomial of t . Then t has two distinct eigenvalues, 1 and -1 , and so the product of the eigenvalues of t is -1 . But the product of the eigenvalues (counting multiplicities) for an arbitrary square matrix is the determinant of the matrix, and it follows that $\det(t) = -1$. But $t \in SL(2, q)$, and so $\det(t) = 1$, and this contradiction completes the proof. ■

It follows by Theorem 6.11 that a Sylow 2-subgroup of $SL(2, q)$ (for odd q) is either cyclic or generalized quaternion. An elementary argument that shows that the cyclic case can never occur depends on the fact that in a finite field F of odd order q , it is always possible to find elements a and b such that $a^2 + b^2 = -1$. Assuming that a and b satisfy this condition, consider the two matrices:

$$x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}.$$

These clearly have determinant 1, and so they lie in $SL(2, q)$. It is easy to check that $x^2 = -I = y^2$ and that $y^x = -y = y^{-1}$, and it follows that the subgroup $\langle x, y \rangle$ of $SL(2, q)$ is isomorphic to the quaternion group Q_8 . A Sylow 2-subgroup of $SL(2, q)$ cannot be cyclic, therefore, and so it must be generalized quaternion. We mention also that since $|SL(2, 3)| = 24$, a Sylow 2-subgroup of $SL(2, 3)$ is isomorphic to Q_8 .

To see why the equation $a^2 + b^2 = -1$ must have a solution in F , observe that the number of elements of F that have the form $1 + a^2$ is exactly $(q + 1)/2$. (This is so because the map $a \mapsto 1 + a^2$ is two-to-one for nonzero elements of F , and so the image of this map contains $(q - 1)/2$ elements different from 1, for a total of $(q + 1)/2$ elements.) Similarly, there are exactly $(q + 1)/2$ elements of F that have the form $-b^2$, and since the

sum of the cardinalities of these two sets exceeds q , the sets must overlap. It follows that $1 + a^2 = -b^2$ for some choice of $a, b \in F$, as wanted.

Proof of Lemma 7.3. Working by induction on $|L|$, we can assume that P centralizes every proper subgroup of L that it stabilizes. If we choose a prime q dividing $|L : \mathbf{C}_L(P)|$, we can find a P -invariant Sylow q -subgroup Q of L , and since $Q \not\subseteq \mathbf{C}_L(P)$, we must have $Q = L$, and thus L is a q -group. Also, $[L, P]$ is P -invariant, and so if $[L, P] < L$, we have $[L, P, P] = 1$, and since $[L, P, P] = [L, P]$ by Lemma 4.29, we conclude that $[L, P] = 1$, as required. We may assume, therefore, that $[L, P] = L$, and in particular, $L \subseteq G' \subseteq SL(2, p)$, where the second containment follows because $GL(2, p)/SL(2, p)$ is isomorphic to the multiplicative group of the field of order p , and so it is abelian.

If $q = 2$, then by assumption, the 2-group L is abelian, and we know by Lemma 7.4 that L contains a unique involution. It follows that L is a cyclic 2-group, and so $\text{Aut}(L)$ is also a 2-group, and the p -group P cannot act nontrivially on L . We can assume, therefore, that q is an odd prime, and since $|L|$ is a power of q that divides $|SL(2, p)| = p(p-1)(p+1)$, it follows that $|L|$ divides one of $p-1$ or $p+1$. (This, of course, is because the prime q cannot divide both $p-1$ and $p+1$.) In particular, we have $|L| \leq p+1$. Now if P acts nontrivially on L , there must be at least one P -orbit in L of size at least p , and together with the identity, this yields $|L| \geq p+1$. We conclude that $|L| = p+1$, and so $|L|$ is even. But $|L|$ is a power of the odd prime q , and this contradiction completes the proof. ■

Next, we prove what we call the “normal- P theorem”.

7.5. Theorem. *Let $P \in \text{Syl}_p(G)$, where G is a finite group, and assume the following conditions.*

- (1) G is p -solvable.
- (2) $p \neq 2$.
- (3) A Sylow 2-subgroup of G is abelian.
- (4) G acts faithfully on some p -group V .
- (5) $|V : \mathbf{C}_V(P)| \leq p$.

Then $P \triangleleft G$.

The reader may wonder how Theorem 7.5, which applies only to p -solvable groups, can possibly be relevant to the proof of Thompson’s theorem (7.1), where there certainly is no p -solvability assumption. The answer is that the proof of Theorem 7.1 proceeds via a subtle induction that will guarantee p -solvability when we need it. (Thompson’s inductive argument

will also guarantee that the Sylow 2-subgroup is abelian when that fact is needed.)

Proof of Theorem 7.5. Assume that G is a counterexample of minimum possible order. Then G does not have a normal Sylow p -subgroup, and we can choose $Q \in \text{Syl}_p(G)$ with $Q \neq P$. The subgroup $\langle Q, P \rangle$ of G has at least two Sylow p -subgroups, and it clearly satisfies all five hypotheses of the theorem. It too is a counterexample, therefore, and so by the minimality of G , we have $G = \langle P, Q \rangle$.

Now $Q = P^g$ for some element $g \in G$, and thus $\mathbf{C}_V(Q) = (\mathbf{C}_V(P))^g$ also has index at most p in V . Let $U = \mathbf{C}_V(P) \cap \mathbf{C}_V(Q)$, and observe that $|V : U| \leq |V : \mathbf{C}_V(P)| |V : \mathbf{C}_V(Q)| \leq p^2$, and $U \triangleleft V$. Also, since both P and Q act trivially on U , it follows that the action of $G = \langle P, Q \rangle$ on U is trivial, and so $[U, G] = 1$. In particular, U is G -invariant, and we have a natural action of G on V/U .

Let K be the kernel of the action of G on V/U , so that $[V, K] \subseteq U$, and thus $[V, K, K] \subseteq [U, K] = 1$. Since V is a p -group, it follows that K must also be a p -group. (If Q is a Sylow q -subgroup of K , where $q \neq p$, then $[V, Q] = [V, Q, Q] = 1$, and thus $Q = 1$ since the action of G on V is faithful, by assumption.) Since $K \subseteq \mathbf{O}_p(G)$, it follows that $K \subseteq P$ and $K \subseteq Q$, and thus the group $\overline{G} = G/K$ has distinct Sylow p -subgroups \overline{P} and \overline{Q} . Also, \overline{G} acts faithfully on V/U , and we see that \overline{P} centralizes $\mathbf{C}_V(P)/U$, which has index $|V : \mathbf{C}_V(P)| \leq p$ in V/U . It follows that the group \overline{G} satisfies all five conditions with respect to its Sylow p -subgroup \overline{P} and its action on V/U , but it does not have a normal Sylow p -subgroup. By the minimality of G , therefore, we must have $K = 1$, and so G acts faithfully on V/U . We can thus replace V by V/U and assume that $|V| \leq p^2$.

Since G acts faithfully on V , it is isomorphically embedded in $\text{Aut}(V)$. If V is cyclic, then $\text{Aut}(V)$ is abelian, and so G is abelian and $P \triangleleft G$, which is not the case. We conclude that V is noncyclic, and so it must be elementary abelian of order p^2 , and thus $\text{Aut}(V) \cong GL(2, p)$, and we can view G as a subgroup of $GL(2, p)$. In particular, $|P| \leq p$, and since P is not normal, it follows that $\mathbf{O}_p(G) = 1$. Now let $L = \mathbf{O}_{p'}(G)$, so that P normalizes the p' -group L . Since we are assuming that a Sylow 2-subgroup of G is abelian, the same is true for L , and thus by Lemma 7.3, we see that P acts trivially on L . By the Hall-Higman Lemma 1.2.3 (our Theorem 3.21) we have $P \subseteq \mathbf{C}_G(L) \subseteq L$, and thus since P is a p -group and L is a p' -group, we have $P = 1$. This is a contradiction since P is not normal. ■

Problems 7A

7A.1. Show that a nilpotent maximal subgroup of a simple group must be a 2-group.

Note. The simple group $PSL(2, 17)$ has a maximal subgroup of order 16, so nontrivial 2-groups actually can occur as maximal subgroups of simple groups.

7A.2. Let $S = SL(2, 3)$ and write $Z = \langle -I \rangle$, so that Z is the unique subgroup of order 2 in S . Show that the group S/Z of order 12 has four Sylow 3-subgroups, and deduce that it has a unique Sylow 2-subgroup. Conclude from this that S has a normal subgroup of order 8.

Hint. Use the fact mentioned in the text that if $n \geq 2$ and q is a power of the prime p , then $GL(n, q)$ has at least two Sylow p -subgroups. No further matrix computations are required for this problem.

7A.3. Let $G = GL(n, q)$, where q is a power of the prime p , and let P be the Sylow p -subgroup of G consisting of the upper triangular matrices with ones on the diagonal. Let D be the group of all diagonal matrices in G .

- (a) Show that $D \subseteq N_G(P)$.
- (b) Show that DP is the group of all upper triangular matrices in G with arbitrary nonzero entries on the diagonal.
- (c) View G as acting by right multiplication on the space of n -dimensional row vectors over the field F of order q . Identify all P -invariant subspaces of V , and observe that there is exactly one such subspace of dimension k for each integer k with $1 \leq k \leq n$.
- (d) Show that all of the P -invariant subspaces of V are N -invariant, where $N = N_G(P)$, and use (c) to deduce that $N = DP$.

7A.4. If q is a power of the prime p , show that $SL(2, q)$ and $PSL(2, q)$ each have exactly $q + 1$ Sylow p -subgroups.

7A.5. Let P be a p -group, and suppose that $U \triangleleft P$ is elementary abelian. Show that U normalizes some group $E \in \mathcal{E}(P)$.

Hint. Choose $E \in \mathcal{E}(P)$ such that $|U \cap E|$ is as large as possible. If U does not normalize E , write $F = E^u$, where $u \in U$ and $E \neq F$. Let $H = \langle E, F \rangle$ and $Z = E \cap F$. Show that $Z(H \cap U) \in \mathcal{E}(P)$.

7A.6. Suppose that Q is a generalized quaternion group and that $|\text{Aut}(Q)|$ is divisible by an odd prime p . Show that $p = 3$ and $|Q| = 8$, and deduce that the hypothesis that a Sylow 2-subgroup is abelian in Lemma 7.3 and Theorem 7.5 is unnecessary if $p > 3$.

7B

In this section, we prove the following “normal-J theorem”. This will be used for the proof of Theorem 7.1, and also for the group-theoretic proof of Burnside’s $p^a q^b$ -theorem.

7.6. Theorem. *Let $P \in \text{Syl}_p(G)$, where G is a finite group, and assume the following conditions.*

- (1) G is p -solvable.
- (2) $p \neq 2$.
- (3) A Sylow 2-subgroup of G is abelian.
- (4) $\mathbf{O}_{p'}(G) = 1$.
- (5) $P = \mathbf{C}_G(\mathbf{Z}(P))$.

Then $\mathbf{J}(P) \triangleleft G$.

Since we are assuming that G is p -solvable and that $\mathbf{O}_{p'}(G) = 1$, it follows (assuming that G is nontrivial) that $\mathbf{O}_p(G) > 1$. The point of the theorem, however, is not simply that G has a nontrivial normal p -subgroup; it is that a *particular* p -subgroup, namely $\mathbf{J}(P)$, is normal in G . Note that it is not until Step 7 of the following proof that we use the actual definition of the set $\mathcal{E}(P)$.

Proof of Theorem 7.6. Suppose that the theorem is false, and let G be a counterexample of minimum possible order. In particular, G is nontrivial, so $\mathbf{O}_p(G) > 1$, and we write $U = \mathbf{O}_p(G)$ and $\bar{G} = G/U$. Also, let $\bar{L} = \mathbf{O}_{p'}(\bar{G})$, where $L \supseteq U$. (This, of course, unambiguously defines the subgroup $L \triangleleft G$.) We proceed in a number of steps, the first of which consists of three closely related statements, all of which are consequences of the Hall-Higman Lemma 1.2.3.

Step 1.

- (a) $\mathbf{Z}(P) \subseteq U$.
- (b) If $U \subseteq H \subseteq G$, then $\mathbf{O}_{p'}(H) = 1$.
- (c) $\mathbf{C}_{\bar{G}}(\bar{L}) \subseteq \bar{L}$.

Proof. Since G is p -solvable and $\mathbf{O}_{p'}(G) = 1$, Lemma 1.2.3 (our Theorem 3.21) tells us that $U = \mathbf{O}_p(G) \supseteq \mathbf{C}_G(U)$. But $U \subseteq P$, and so $\mathbf{Z}(P) \subseteq \mathbf{C}_G(U)$ and (a) follows. Also, since $U = \mathbf{O}_p(G)$, we see that $\mathbf{O}_p(\bar{G}) = 1$, and Lemma 1.2.3 yields (c). For (b), let $U \subseteq H \subseteq G$ and write $M = \mathbf{O}_{p'}(H)$. Then M and U are normal in H and $M \cap U = 1$ since U is a p -group and M is a p' -group. Thus $M \subseteq \mathbf{C}_G(U) \subseteq U$, so $M = M \cap U = 1$, proving (b).

Step 2. There exists $A \in \mathcal{E}(P)$ such that $A \not\subseteq U$.

Proof. Otherwise, all members of $\mathcal{E}(P)$ are contained in U , and thus $\mathbf{J}(P) \subseteq U$. It follows by Lemma 7.2 that $\mathbf{J}(P) = \mathbf{J}(U)$ is characteristic in U , and since $U \triangleleft G$, we have $\mathbf{J}(P) \triangleleft G$. This is a contradiction since we are assuming that G is a counterexample.

Step 3. Let $UA \subseteq H < G$, and suppose that $H \cap P \in \text{Syl}_p(H)$. Then \overline{A} centralizes $\overline{H \cap L}$.

Proof. Observe that H satisfies the first four hypotheses of the theorem. First, H is p -solvable since it is a subgroup of the p -solvable group G . Also, p is still different from 2, so the second condition holds. A Sylow 2-subgroup of H is contained in a Sylow 2-subgroup of G , which is abelian, and so H satisfies condition (3), and finally, $\mathbf{O}_{p'}(H) = 1$ by Step 1(b).

Now let $S = H \cap P \in \text{Syl}_p(H)$. Since $\mathbf{Z}(P) \subseteq U \subseteq S \subseteq P$ by Step 1(a), we have $\mathbf{Z}(P) \subseteq \mathbf{Z}(S)$, and thus $\mathbf{C}_H(\mathbf{Z}(S)) \subseteq \mathbf{C}_G(\mathbf{Z}(P)) = P$. Thus $\mathbf{C}_H(\mathbf{Z}(S))$ is a p -subgroup of H containing the Sylow p -subgroup S , and so $\mathbf{C}_H(\mathbf{Z}(S)) = S$ and H satisfies the fifth hypothesis too.

Since $H < G$, the theorem holds for H , and hence $\mathbf{J}(S) \triangleleft H$. Also, since $A \in \mathcal{E}(P)$ and $A \subseteq S \subseteq P$, it follows that $A \in \mathcal{E}(S)$, and so $A \subseteq \mathbf{J}(S)$. Then

$$[H \cap L, A] \subseteq [H \cap L, \mathbf{J}(S)] \subseteq (H \cap L) \cap \mathbf{J}(S) = L \cap \mathbf{J}(S) \subseteq U,$$

where the second containment holds because both $H \cap L$ and $\mathbf{J}(S)$ are normal in H , and the final containment holds because U is the unique Sylow p -subgroup of L , and thus it contains every p -subgroup of L . We now have $1 = [\overline{H \cap L}, \overline{A}] = [\overline{H \cap L}, \overline{A}]$, as wanted.

Step 4. $G = LA$ and $P = UA$.

Proof. Write $H = LA$, and observe that UA is a p -subgroup of H and that $|H : UA| = |L(UA) : UA| = |L : L \cap UA|$, which divides the p' -number $|L : U|$. It follows that $UA \in \text{Syl}_p(H)$, and thus $UA = H \cap P$. If $H < G$, then since $L \subseteq H$, Step 3 yields $\overline{A} \subseteq \mathbf{C}_{\overline{G}}(\overline{L}) \subseteq \overline{L}$, where the second containment holds by Step 1(c). Since \overline{A} is a p -group and \overline{L} is a p' -group, we have $\overline{A} = 1$, and so $A \subseteq U$. This contradicts the choice of A , however, and we conclude that $H = G$, as wanted. Finally, we have $UA = H \cap P = G \cap P = P$.

Step 5. $|\overline{A}| = p$.

Proof. First, \overline{A} is nontrivial since $A \not\subseteq U$. Also, \overline{A} is elementary abelian, and so it suffices to show that it is cyclic. Now \overline{A} acts coprimely on \overline{L} , and this action is faithful since $\mathbf{C}_{\overline{G}}(\overline{L}) \subseteq \overline{L}$ and $\overline{L} \cap \overline{A} = 1$. By Lemma 6.20,

therefore, it suffices to show that \overline{A} acts trivially on every \overline{A} -invariant proper subgroup of \overline{L} .

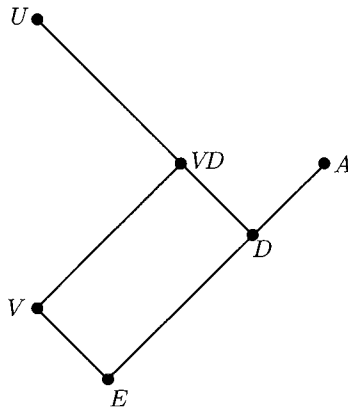
Suppose that \overline{M} is \overline{A} -invariant, where $\overline{M} < \overline{L}$, and where we assume (as we may) that $M \supseteq U$. Then $A \subseteq \mathbf{N}_G(M)$, and so MA is a group, and $MA \supseteq UA = P$. Also, since A is a p -group, the p' -part of $|MA|$ is equal to the p' -part of $|M|$, and this is strictly less than the p' -part of $|L|$ since $|L : M|$ is a p' -number exceeding 1. It follows that $MA < G$, and we can apply Step 3 to deduce that \overline{A} centralizes $\overline{MA \cap L} \supseteq \overline{M}$, proving Step 5.

Now let $V = \{z \in \mathbf{Z}(U) \mid z^p = 1\}$, so that V is an elementary abelian normal subgroup of G . Then G acts by conjugation on V , and since $V \subseteq \mathbf{Z}(U)$, we see that U acts trivially. This yields an action of $\overline{G} = G/U$ on V .

Step 6. The action of \overline{G} on V is faithful.

Proof. Let $K = \mathbf{C}_G(V)$, so that \overline{K} is the kernel of the action of \overline{G} on V . We argue that K is a p -group by considering a Sylow q -subgroup Q of K , where q is any prime different from p . Then Q acts coprimely on the abelian group $\mathbf{Z}(U)$, and Q fixes all elements of order p in $\mathbf{Z}(U)$ since these elements all lie in V and $Q \subseteq K = \mathbf{C}_G(V)$. It follows by Corollary 4.35 that Q acts trivially on $\mathbf{Z}(U)$. But $\mathbf{Z}(P) \subseteq U$, and so $\mathbf{Z}(P) \subseteq \mathbf{Z}(U)$, and thus $Q \subseteq \mathbf{C}_G(\mathbf{Z}(P)) = P$. We conclude that $Q = 1$, and thus K is a p -group, as claimed. But $K \triangleleft G$, so $K \subseteq \mathbf{O}_p(G) = U$, and thus $\overline{K} = 1$, as wanted.

Step 7. $|V : V \cap A| \leq p$.



Proof. Write $D = U \cap A$ and $E = V \cap A$ as in the diagram, and observe that $|V : E| = |V : V \cap D| = |VD : D|$. Now D is an elementary abelian subgroup of U , and V is a central elementary abelian subgroup of U , and thus VD is elementary abelian. Since $A \in \mathcal{E}(P)$, it follows that $|VD| \leq |A|$, and thus $|VD : D| \leq |A : D| = |\bar{A}| = p$. We now have $|V : E| = |VD : D| \leq p$, as wanted.

Step 8. We have a contradiction.

We want to apply the “normal- P theorem” (Theorem 7.5) to the faithful action of \bar{G} on V , and so we need to check that $|V : \mathbf{C}_V(\bar{P})| \leq p$. But $P = UA$, so $\bar{P} = \bar{A}$, and of course, \bar{A} centralizes $V \cap A$ since A is abelian. Thus $|V : \mathbf{C}_V(\bar{P})| \leq |V : V \cap A| \leq p$, as wanted, and we conclude that $\bar{P} \triangleleft \bar{G}$. Then $P \triangleleft G$ and $A \subseteq P \subseteq \mathbf{O}_p(G) = U$, which is not the case. ■

7C

In this section, we prove Theorem 7.1, thereby completing the proof that Frobenius kernels are nilpotent. We begin with an extension of Lemma 2.17.

7.7. Lemma. *Write $\bar{G} = G/N$, where N is a normal p' -subgroup of a finite group G . If P is a p -subgroup of G , we have*

- (a) $\mathbf{N}_{\bar{G}}(\bar{P}) = \overline{\mathbf{N}_G(P)}$ and
- (b) $\mathbf{C}_{\bar{G}}(\bar{P}) = \overline{\mathbf{C}_G(P)}$.

Proof. Statement (a) is essentially Lemma 2.17. Also, since overbar is a homomorphism, it is clear that $\overline{\mathbf{C}_G(P)} \subseteq \mathbf{C}_{\bar{G}}(\bar{P})$, and so to establish (b), it suffices to prove the reverse containment. By (a), overbar defines a surjective homomorphism from $\mathbf{N}_G(P)$ to $\mathbf{N}_{\bar{G}}(\bar{P})$, and so by the correspondence theorem, the subgroup $\mathbf{C}_{\bar{G}}(\bar{P}) \subseteq \mathbf{N}_{\bar{G}}(\bar{P})$ is the image of some subgroup $X \subseteq \mathbf{N}_G(P)$. In other words, $\bar{X} = \mathbf{C}_{\bar{G}}(\bar{P})$, and we have $1 = [\bar{P}, \bar{X}] = \overline{[P, X]}$, and thus $[P, X] \subseteq N$. But $X \subseteq \mathbf{N}_G(P)$, and so we also have $[P, X] \subseteq P$. Thus $\overline{[P, X]} \subseteq N \cap P = 1$, and $X \subseteq \mathbf{C}_G(P)$. We conclude that $\mathbf{C}_{\bar{G}}(\bar{P}) = \overline{X} \subseteq \overline{\mathbf{C}_G(P)}$, and the proof is complete. ■

We are now ready to prove Theorem 7.1, which, we recall, asserts that G has a normal p -complement if $p \neq 2$ and both $\mathbf{N}_G(\mathbf{J}(P))$ and $\mathbf{C}_G(\mathbf{Z}(P))$ have normal p -complements, where P is a Sylow p -subgroup of G . (Of course, if these conditions hold for P , they will also hold for every Sylow p -subgroup of G .) We repeatedly use the fact that the property of having a normal p -complement is inherited by subgroups and homomorphic images.

Observe the subtle way that the subgroup U is chosen in the following proof. This is one of the keys to this very clever argument. (This trick appears both in Thompson's thesis and in his 1964 paper.)

Proof of Theorem 7.1. Suppose that G is a counterexample of minimal order. Then G fails to have a normal p -complement, and so by Frobenius' theorem (Theorem 5.26), there must be some nonidentity p -subgroup U of G such that $\mathbf{N}_G(U)$ fails to have a normal p -complement. Among all such "bad" subgroups, choose U such that $|\mathbf{N}_G(U)|_p$ is as large as possible. (In other words, U is chosen so that a Sylow p -subgroup of $\mathbf{N}_G(U)$ has order as large as possible.) Subject to that condition, choose U to have order as large as possible. We proceed in a number of steps.

Step 1. $U = \mathbf{O}_p(G)$.

Proof. Let $S \in \text{Syl}_p(N)$, where $N = \mathbf{N}_G(U)$, and suppose that $N < G$. Then N is not a counterexample to the theorem, and since N fails to have a normal p -complement, at least one of $\mathbf{N}_N(\mathbf{J}(S))$ or $\mathbf{C}_N(\mathbf{Z}(S))$ must fail to have a normal p -complement. Then one of $\mathbf{N}_G(\mathbf{J}(S))$ or $\mathbf{C}_G(\mathbf{Z}(S))$ fails to have a normal p -complement, and so by hypothesis, S cannot be a full Sylow p -subgroup of G . Then S is properly contained in a Sylow p -subgroup, and hence we can choose a p -subgroup T such that $S \triangleleft T$ and $S < T$. (We are, of course, using the fact that "normalizers grow" in p -groups.)

Now $\mathbf{N}_G(X)$ fails to have a normal p -complement, where X is one of $\mathbf{J}(S)$ or $\mathbf{Z}(S)$. Also $U > 1$, so $S > 1$, and thus $X > 1$, and therefore X is a member of the set of bad subgroups from which we selected U . Also, X is characteristic in S , and so $X \triangleleft T$ and $T \subseteq \mathbf{N}_G(X)$. We thus have $|\mathbf{N}_G(X)|_p \geq |T| > |S| = |\mathbf{N}_G(U)|_p$, and since this contradicts the choice of U , we conclude that $N = G$, and so $U \triangleleft G$ and $U \subseteq \mathbf{O}_p(G)$. Now $\mathbf{O}_p(G)$ is a member of the set of nonidentity p -subgroups whose normalizers fail to have normal p -complements, and since $|\mathbf{N}_G(\mathbf{O}_p(G))|_p = |P| = |\mathbf{N}_G(U)|_p$, the choice of U guarantees that $|U| \geq |\mathbf{O}_p(G)|$, and thus $U = \mathbf{O}_p(G)$, as required.

Step 2. G/U has a normal p -complement, and so G is p -solvable.

Proof. Write $\overline{G} = G/U$, and observe that $|\overline{G}| < |G|$. Then \overline{G} is not a counterexample to the theorem, and so since $\overline{P} \in \text{Syl}_p(\overline{G})$, it suffices to show that each of $\mathbf{N}_{\overline{G}}(\mathbf{J}(\overline{P}))$ and $\mathbf{C}_{\overline{G}}(\mathbf{Z}(\overline{P}))$ has a normal p -complement. There is nothing to prove if p does not divide $|\overline{G}|$, and so we can assume that \overline{P} is nontrivial, and thus $\mathbf{J}(\overline{P})$ and $\mathbf{Z}(\overline{P})$ are nontrivial. Let $U \subseteq X \subseteq P$, where \overline{X} is either $\mathbf{J}(\overline{P})$ or $\mathbf{Z}(\overline{P})$, and observe that $X > U$. Also, $X \triangleleft P$, and so $P \subseteq \mathbf{N}_G(X)$ and $|\mathbf{N}_G(X)|_p = |P| = |\mathbf{N}_G(U)|_p$. But $|X| > |U|$, and so by the choice of U , we see that X cannot be one of the bad subgroups whose

normalizers fail to have normal p -complements. Since X contains the kernel U of overbar, we have $\mathbf{N}_{\overline{G}}(\overline{X}) = \overline{\mathbf{N}_G(X)}$ by the correspondence theorem, and thus $\mathbf{N}_{\overline{G}}(\overline{X})$ has a normal p -complement. In particular, both $\mathbf{N}_{\overline{G}}(\mathbf{J}(\overline{P}))$ and $\mathbf{N}_{\overline{G}}(\mathbf{Z}(\overline{P}))$ have normal p -complements, and therefore, \overline{G} has a normal p -complement, as required.

Step 3. $\mathbf{O}_{p'}(G) = 1$.

Proof. Let $K = \mathbf{O}_{p'}(G)$, and write $\overline{G} = G/K$. Now \overline{P} is a Sylow p -subgroup of \overline{G} , and since K is a p' -group, overbar defines an isomorphism from P onto \overline{P} . It follows that $\overline{\mathbf{J}(P)} = \mathbf{J}(\overline{P})$ and $\overline{\mathbf{Z}(P)} = \mathbf{Z}(\overline{P})$. Then

$$\begin{aligned}\mathbf{N}_{\overline{G}}(\mathbf{J}(\overline{P})) &= \mathbf{N}_{\overline{G}}(\overline{\mathbf{J}(P)}) = \overline{\mathbf{N}_G(\mathbf{J}(P))} \quad \text{and} \\ \mathbf{C}_{\overline{G}}(\mathbf{Z}(\overline{P})) &= \mathbf{C}_{\overline{G}}(\overline{\mathbf{Z}(P)}) = \overline{\mathbf{C}_G(\mathbf{Z}(P))},\end{aligned}$$

where the second equality in each of these equations follows by Lemma 7.7. We conclude that $\mathbf{N}_{\overline{G}}(\mathbf{J}(\overline{P}))$ and $\mathbf{C}_{\overline{G}}(\mathbf{Z}(\overline{P}))$ have normal p -complements, and so if $|\overline{G}| < |G|$, it would follow that \overline{G} has a normal p -complement. This is not the case, however, since $K = \mathbf{O}_{p'}(G)$ and G fails to have a normal p -complement. Then $|\overline{G}|$ is not smaller than $|G|$, and so $K = 1$, as required.

Step 4. P is a maximal subgroup of G .

Proof. Suppose that $P \subseteq H < G$. Then $\mathbf{N}_H(\mathbf{J}(P))$ and $\mathbf{C}_H(\mathbf{Z}(P))$ have normal p -complements, and since H is not a counterexample, it follows that H has a normal p -complement K . Then $K \triangleleft H$ and $\mathbf{O}_p(G) \triangleleft H$, and since $K \cap \mathbf{O}_p(G) = 1$, we have $K \subseteq \mathbf{C}_G(\mathbf{O}_p(G)) \subseteq \mathbf{O}_p(G)$. (We are using Lemma 1.2.3, which applies because G is p -solvable by Step 2 and $\mathbf{O}_{p'}(G) = 1$ by Step 3.) Then $K = 1$ and H is a p -group, and hence $H = P$.

Step 5. $\mathbf{C}_G(\mathbf{Z}(P)) = P$.

Proof. Certainly, $\mathbf{C}_G(\mathbf{Z}(P)) \supseteq P$. But $\mathbf{C}_G(\mathbf{Z}(P)) < G$ since G fails to have a normal p -complement, and thus $\mathbf{C}_G(\mathbf{Z}(P)) = P$ by Step 4.

Step 6. The normal p -complement of G/U is abelian.

Proof. First, recall that G/U has a normal p -complement L/U by Step 2. Suppose that $U \subseteq X \subseteq L$, where X is normalized by P . Then PX is a group, and hence by Step 4, either $PX = P$ or $PX = G$. If $PX = P$, then $|X|$ is a power of p , and so $X = U$. If, on the other hand, $PX = G$, then $|G : X|$ is a power of p , and hence $X = L$. It follows that no nonidentity proper subgroup of $\overline{L} = L/U$ is P -invariant.

We can certainly assume that \bar{L} is nontrivial, and so it has a nontrivial P -invariant Sylow q -subgroup for some prime q . It follows from the result of the previous paragraph that \bar{L} is a q -group, and since it is nontrivial, we have $(\bar{L})' < \bar{L}$. Of course, $(\bar{L})'$ is P -invariant, and thus $(\bar{L})' = 1$, and it follows that \bar{L} is abelian.

Step 7. We have a contradiction.

Proof. We argue that G satisfies all five hypotheses of the normal-J theorem (Theorem 7.6). Certainly, $p \neq 2$, and we know that G is p -solvable, that $\mathbf{O}_{p'}(G) = 1$, and that $P = \mathbf{C}_G(\mathbf{Z}(P))$. All that remains, therefore, is to check that a Sylow 2-subgroup of G is abelian.

Write $\bar{G} = G/U$ and let $Q \in \text{Syl}_2(G)$, so that \bar{Q} is a p' -subgroup of \bar{G} , and thus \bar{Q} is contained in the abelian normal p -complement of \bar{G} . (We are using Step 6 here.) Also, $Q \cong \bar{Q}$ because U is the kernel of the canonical homomorphism $G \rightarrow \bar{G}$ and $Q \cap U = 1$, and thus Q is abelian, as wanted. By Theorem 7.6, therefore, $\mathbf{J}(P) \triangleleft G$. But then $G = \mathbf{N}_G(\mathbf{J}(P))$ has a normal p -complement, and this is our final contradiction. ■

Problems 7C

7C.1. (Thompson) Let $P \in \text{Syl}_p(G)$, where G is finite and $p \neq 2$, and suppose that $\mathbf{N}_G(X)/\mathbf{C}_G(X)$ is a p -group for every characteristic subgroup X of P . Show that G has a normal p -complement.

Hint. Work by induction on $|G|$ and use the inductive hypothesis to show that if X is characteristic in P and $X > 1$, then $\mathbf{N}_G(X)$ has a normal p -complement.

7D

In this section, we prove Burnside's theorem.

7.8. Theorem. *Let G be a finite group of order $p^a q^b$, where p and q are primes. Then G is solvable.*

Burnside's proof of this theorem was one of the first major applications of character theory, early in the 20th century. (Characters were invented by Frobenius, who used them to prove his theorem on the existence of Frobenius kernels, but Burnside was one of the early developers of the theory.) Burnside's proof appears in the second (1911) edition of his group theory text, of which a very substantial fraction is devoted to character and linear representation theory. It is interesting that the first (1897) edition of Burnside's book includes no character theory at all, apparently because he

felt that it was not good for much. Burnside wrote in his preface to the first edition that “it would be difficult to find a result that could be most directly obtained by the consideration of [linear representations].” He began the preface to the second edition with the assertion that “Very considerable advances ... have been made since the appearance of the first edition of this book.” (Was he thinking primarily of his own $p^a q^b$ -theorem?) In fact, Burnside’s proof is elegant and not very difficult; it lies relatively near the surface of character theory, and it appears fairly early in most modern texts on the subject. Nevertheless, it has always seemed somewhat strange that one had to use facts about the field of complex numbers in order to prove this theorem about finite groups.

By the late 1960s, considerable advances (to use Burnside’s words) had been made in pure finite group theory. In particular, the Thompson subgroup, and Thompson’s techniques of “local analysis” had been developed, and these had proved to be very powerful tools, as we have seen in this chapter. Thompson’s Ph.D. student David Goldschmidt wondered whether or not these tools could be used to give a non-character proof of Burnside’s theorem. (The real point here was to demonstrate the power of Thompson’s techniques; no one claimed that there was any deficiency in Burnside’s elegant proof.)

Goldschmidt almost succeeded: he was able to prove the $p^a q^b$ -theorem provided that both p and q are different from 2. A few years later, and approximately simultaneously, H. Bender and H. Matsuyama found ways to handle the remaining case. Matsuyama’s argument was easier, but Bender’s approach, when supplemented by Matsuyama’s idea, yielded an overall simplification of Goldschmidt’s argument, and that is essentially the proof we present here. (But Bender used Glauberman’s $\mathbf{Z}(J)$ -theorem, which we have decided not to include in this book. Instead, we appeal to the normal- J theorem.)

Proof of Theorem 7.8. Let G be a counterexample of smallest possible order. Since the order of every proper subgroup of G also has at most two prime divisors, every such subgroup must be solvable, and also if $1 < N \triangleleft G$, then G/N is solvable. In particular, if N is a nontrivial proper normal subgroup of G , then both N and G/N are solvable, and hence G is solvable, which contradicts our assumption that G is a counterexample. It follows that G is simple.

We focus now on the maximal subgroups of G . If K is any nontrivial normal subgroup of a maximal subgroup M , then of course, $M \subseteq \mathbf{N}_G(K)$, and since $1 < K < G$ and G is simple, we know that $\mathbf{N}_G(K) < G$. It follows by the maximality of M that $M = \mathbf{N}_G(K)$. (This observation will be used repeatedly in what follows.) Also, if M is maximal, then M is solvable

and nontrivial, and so it has a nonidentity normal subgroup of prime-power order. Thus either $\mathbf{O}_p(M) > 1$ or $\mathbf{O}_q(M) > 1$, and one of our intermediate goals is to show that it is not possible for both $\mathbf{O}_p(M)$ and $\mathbf{O}_q(M)$ to be nontrivial. We proceed in a number of steps.

Step 1. Suppose that $K \subseteq G$ is nilpotent, and assume that $M = \mathbf{N}_G(K)$ is a maximal subgroup of G . If both p and q divide $|K|$, then M is the unique maximal subgroup of G containing K .

Proof. Assuming that the assertion is false, let K be maximal among counterexample subgroups, and let $K \subseteq X$, where X is a maximal subgroup of G different from M . Write $K = K_p \times K_q$, where K_p and K_q are respectively the (nontrivial) Sylow p -subgroup and Sylow q -subgroup of K . Since K_p is characteristic in K , we have $K_p \triangleleft M$, and it follows that $M = \mathbf{N}_G(K_p)$.

Now $M \cap X = \mathbf{N}_X(K_p)$ is a p -local subgroup of X . Also, $K_q \triangleleft M \cap X$, and so $K_q \subseteq \mathbf{O}_{p'}(K \cap X)$. Since X is solvable and $X \cap M$ is a p -local subgroup of X , we can apply Theorem 4.33 to conclude that $\mathbf{O}_{p'}(M \cap X) \subseteq \mathbf{O}_{p'}(X)$. This yields $K_q \subseteq \mathbf{O}_{p'}(X) = \mathbf{O}_q(X)$, and so writing $L_q = \mathbf{O}_q(X)$, we have $K_q \subseteq L_q$. Similarly, $K_p \subseteq L_p$, where $L_p = \mathbf{O}_p(X)$, and thus both L_p and L_q are nontrivial. Write $L = L_p L_q$, and note that $K \subseteq L$. Also, L is nilpotent, $|L|$ is divisible by both p and q and $X = \mathbf{N}_G(L)$ is a maximal subgroup of G . If $K < L$, it follows by the choice of K that X is the unique maximal subgroup of G that contains L . But $K_p \subseteq L_p$, and thus

$$L_q \subseteq \mathbf{C}_G(L_p) \subseteq \mathbf{C}_G(K_p) \subseteq \mathbf{N}_G(K_p) = M,$$

and similarly, $L_p \subseteq M$. Then $L \subseteq M$, and since X is the unique maximal subgroup containing L , we have $M = X$, which is a contradiction. In the remaining case, $K = L$, and thus $M = \mathbf{N}_G(K) = \mathbf{N}_G(L) = X$, and again we have a contradiction.

Step 2. Let $P \in \text{Syl}_p(G)$, and suppose that P normalizes some nontrivial subgroup V of G . Then $\langle V, Q \rangle = G$ for every Sylow q -subgroup Q of G . In particular, V cannot be a q -group.

Proof. Let $Q \in \text{Syl}_q(G)$, and write $H = \langle V, Q \rangle$. Now $|PQ| = |P||Q| = |G|$ since $P \cap Q = 1$, and thus $PQ = G$. Let g be an arbitrary element of G and write $g = xy$, with $x \in P$ and $y \in Q$. Since P normalizes V , we have $V^g = V^{xy} = V^y \subseteq H$, and thus H contains all G -conjugates of V . It follows that H contains the nonidentity normal subgroup V^G generated by the conjugates of V , and since G is simple, $V^G = G$, and so $H = G$. To prove the final assertion, observe that if V is a q -group, we can choose Q to contain V , and then $\langle V, Q \rangle = Q < G$, contradicting what we have proved.

Step 3. Let M be maximal in G . Then either $\mathbf{O}_p(M) = 1$ or $\mathbf{O}_q(M) = 1$.

Proof. Assume that the assertion is false, and write $Z_p = \mathbf{Z}(\mathbf{O}_p(M))$ and $Z_q = \mathbf{Z}(\mathbf{O}_q(M))$, so that Z_p and Z_q are both nontrivial and normal in M . Also, Z_p and Z_q are abelian, and they centralize each other since they intersect trivially, and thus the group $Z = Z_p Z_q$ is abelian. Furthermore, $Z \triangleleft M$, and so $M = \mathbf{N}_G(Z)$, and it follows by Step 1 that M is the unique maximal subgroup of G that contains Z . Now if $1 \neq z \in Z$, then $Z \subseteq \mathbf{C}_G(z) < G$, and so $\mathbf{C}_G(z)$ is contained in some maximal subgroup of G that contains Z , and we conclude that $\mathbf{C}_G(z) \subseteq M$.

Let $S \in \text{Syl}_p(M)$. Since S normalizes the nontrivial q -subgroup Z_q , it follows by Step 2 that S cannot be a full Sylow p -subgroup of G . Then $S < P$ for some Sylow p -subgroup P of G , and hence $\mathbf{N}_P(S)$ is a p -subgroup of G strictly larger than S . Then $\mathbf{N}_P(S) \not\subseteq M$, and we can choose an element $q \in G - M$ such that $S^q = S$.

Now write $A = (Z_p)^g$, and observe that since $Z_p \subseteq \mathbf{O}_p(M) \subseteq S$, we have $A = (Z_p)^g \subseteq S^g = S \subseteq M$, and thus A acts on the normal subgroup Z_q of M . Suppose either that the action of A on Z_q is not faithful or that A is not cyclic. In both cases, we argue that

$$Z_q = \langle \mathbf{C}_{Z_q}(a) \mid 1 \neq a \in A \rangle.$$

This is clear if the action is not faithful since in that case, there exists a nonidentity element $a \in A$ such that $\mathbf{C}_{Z_q}(a) = Z_q$. If A is not cyclic, then since it is abelian, Theorem 6.20 applies to yield the assertion.

We argued previously that $\mathbf{C}_G(z) \subseteq M$ for all nonidentity elements $z \in Z$. Then $\mathbf{C}_G(z^g) \subseteq M^g$ for all nonidentity elements $z^g \in Z^g$, and in particular, since $A = (Z_p)^g \subseteq Z^g$, we have $\mathbf{C}_G(a) \subseteq M^g$ if $1 \neq a \in A$. If the action of A on Z_q is not faithful or if A is not cyclic, therefore, we deduce that $Z_q \subseteq M^g$. Also $Z_p \subseteq S = S^g \subseteq M^g$, and thus $Z = Z_p Z_q \subseteq M^g$. But M is the unique maximal subgroup containing Z , and therefore $M = M^g$ and we have $g \in \mathbf{N}_G(M) = M$, which is not the case.

We deduce that A is cyclic and that it acts faithfully on Z_q . Also, since $A = (Z_p)^g$, we see that Z_p is cyclic. By similar reasoning, with the roles of p and q interchanged, we deduce that Z_q is cyclic. But A is a nontrivial p -group that acts faithfully on Z_q , and so p divides $|\text{Aut}(Z_q)|$, and since Z_q is cyclic, we see that p divides $q - 1$, and so $p < q$. Exploiting the symmetry between p and q once again, we have $q < p$, and this, of course, is a contradiction, which completes the proof of Step 3.

If M is an arbitrary maximal subgroup of G , we have observed that at least one of $\mathbf{O}_p(M)$ or $\mathbf{O}_q(M)$ is nontrivial, and now by Step 3, we know that exactly one of these subgroups is nontrivial. In other words, G has two flavors of maximal subgroups: those for which $\mathbf{O}_p(M) > 1$ and those for which $\mathbf{O}_q(M) > 1$, and we refer to these as p -type maximals and q -type

maximals, respectively. We stress that every maximal subgroup of G has exactly one of these types.

Before we proceed with the next step, we define a p -central element of G to be a nonidentity element in the center of some Sylow p -subgroup of G , and similarly, a q -central element is a nonidentity element of the center of some Sylow q -subgroup of G .

Step 4. Suppose that $y \in \mathbf{N}_G(V)$, where y is q -central and V is a p -subgroup. Then V contains no p -central elements.

Proof. Given a p -subgroup $U \subseteq G$, write U^* to denote the subgroup generated by the p -central elements in U . Since the G -conjugates of a p -central element are p -central, it follows that $\mathbf{N}_G(U)$ permutes the p -central elements of U , and thus $\mathbf{N}_G(U)$ normalizes U^* . In particular, since y normalizes V , it is also true that y normalizes V^* , and our goal is to show that $V^* = 1$.

Now V^* is a p -subgroup of G that is normalized by y and is generated by p -central elements, and we let W be a p -subgroup of G , maximal subject to the conditions that it is normalized by y and generated by p -central elements. If $V^* > 1$, then $W > 1$, and we work to obtain a contradiction.

Write $N = \mathbf{N}_G(W)$, and let $S \in \text{Syl}_p(N)$ so that $S \supseteq W$. Since y is q -central, we can choose $Q \in \text{Syl}_q(G)$ such that $y \in \mathbf{Z}(Q)$. Then $\langle y \rangle$ is normalized by Q , and since $y \in N$, we have $\langle y, S \rangle \subseteq N < G$, where the strict inequality holds because $1 < W \triangleleft N$.

It follows by Step 2 (with the roles of p and q reversed) that S cannot be a full Sylow p -subgroup of G . Since $S \in \text{Syl}_p(N)$, we can reason as before that $\mathbf{N}_G(S) \not\subseteq N$, and thus there exists an element $g \in G - N$ such that $S^g = S$. In particular, $W^g \neq W$, but $W^g \subseteq S^g = S \subseteq N$.

Since W is generated by p -central elements and $W^g \neq W$, there must be at least one p -central generator x of W such that $x^g \notin W$. Because x is p -central, we can choose $P \in \text{Syl}_p(G)$ such that $x \in \mathbf{Z}(P)$. Now $G = PQ$, and so we can write $g = ab$, with $a \in P$ and $b \in Q$. Then $x^g = x^{ab} = x^b \in W^b$ and $x^g \in W^g \subseteq N$, and thus $x^g \in W^b \cap N$. Since $W^b \cap N$ is a p -subgroup that normalizes the p -group W , it follows that $W(W^b \cap N)$ is a p -subgroup of G . Also, $W = W^*$, and so $(W(W^b \cap N))^* \supseteq \langle W, x^g \rangle > W$.

Now W^b is normalized by $y^b = y$. Since $y \in N$, it follows that $W^b \cap N$ is normalized by y , and therefore $(W(W^b \cap N))^*$ is a p -subgroup that is normalized by y . This subgroup is generated by p -central elements and it strictly contains W , contradicting the choice of W .

Step 5. Every p subgroup of G is centralized by a p -central element. Also, p -type maximal subgroups of G contain no q -central elements.

Proof. Given a p -subgroup $V \subseteq G$, choose $P \in \text{Syl}_p(G)$ with $P \supseteq V$. Then $\mathbf{Z}(P) \subseteq \mathbf{C}_G(V)$, and so $\mathbf{C}_G(V)$ contains a p -central element.

Now suppose that M is a p -type maximal subgroup, and let $V = \mathbf{O}_p(M)$, so that $V > 1$ and $\mathbf{O}_q(M) = 1$ by Step 3. Then $V \supseteq \mathbf{C}_M(V) = \mathbf{C}_G(V)$ by the Hall-Higman Lemma 1.2.3, and thus V contains a p -central element. By Step 4, no q -central element lies in $\mathbf{N}_G(V) = M$, as required.

Step 6. A q -central element of G cannot normalize a nontrivial p -subgroup.

Proof. Let V be a nontrivial p -subgroup of G , and let M be a maximal subgroup of G containing $\mathbf{N}_G(V)$. It follows by Step 5 that M contains a p -central element, and thus by Step 5 again, with p and q interchanged, M cannot have q -type, and thus it has p -type. By Step 5 yet again, M cannot contain a q -central element, and in particular, $\mathbf{N}_G(V)$ contains no q -central element.

Step 7. $p \neq 2$ and $q \neq 2$.

Proof. Suppose $q = 2$ and choose an involution t in the center of a Sylow q -subgroup. By Theorem 2.13, there exists an element $x \in G$ of order p such that $x^t = x^{-1}$, and thus $t \in \mathbf{N}_G(\langle x \rangle)$. Since t is q -central, however, this contradicts Step 6. We deduce that $q \neq 2$, and, similarly, $p \neq 2$.

Step 8. Let M be a p -type maximal subgroup of G , and let $S \in \text{Syl}_p(M)$. Then $\mathbf{J}(S) \triangleleft M$ and S is a full Sylow p -subgroup of G .

Proof. We wish to apply the normal-J theorem (Theorem 7.6) to the group M , and so we proceed to check the five hypotheses. First, M is solvable, and so it is certainly p -solvable. By Step 7, we know that $p \neq 2$ and that a Sylow 2-subgroup of M is trivial, and hence is abelian, and thus the second and third hypotheses hold. Since M has p -type, we know that $\mathbf{O}_{p'}(M) = \mathbf{O}_q(M) = 1$, and the fourth condition holds.

The remaining condition is that $\mathbf{C}_M(\mathbf{Z}(S)) = S$, and to establish this, it suffices to show that $\mathbf{C}_M(\mathbf{Z}(S))$ is a p -group. Otherwise, $\mathbf{C}_M(\mathbf{Z}(S))$ contains some subgroup Y of order q , and thus $\mathbf{Z}(S)$ normalizes Y . This will contradict Step 6 (with p and q interchanged) if we can show that $\mathbf{Z}(S)$ contains a p -central element.

Let $S \subseteq P \in \text{Syl}_p(G)$, and observe that $S = M \cap P$. Since M is a p -type maximal subgroup, we can write $M = \mathbf{N}_G(V)$ for some p -subgroup V , and we have $V \subseteq S \subseteq P$. Then $\mathbf{Z}(P) \subseteq \mathbf{N}_G(V) \cap P = M \cap P = S$, and it follows that $\mathbf{Z}(P) \subseteq \mathbf{Z}(S)$. Thus $\mathbf{Z}(S)$ contains p -central elements, and so $\mathbf{C}_M(\mathbf{Z}(S)) = S$, as wanted. We see now that M satisfies the hypotheses of the normal-J theorem, so we have $\mathbf{J}(S) \triangleleft M$.

Finally, if S is not a full Sylow p -subgroup of M , we can write $S \triangleleft T$, where T is a p -subgroup of G properly containing S . Then $T \subseteq \mathbf{N}_G(\mathbf{J}(S)) = M$, and this is a contradiction since $T > S$ and S is a full Sylow p -subgroup of M .

Step 9. We have a contradiction.

Proof. Of course, the p -part and the q -part of $|G|$ are unequal, and so we can assume that $|G|_p > |G|_q$. If $S, T \in \text{Syl}_p(G)$, therefore, we have

$$|G_p|^2 > |G_p||G_q| = |G| \geq |ST| = \frac{|S||T|}{|S \cap T|} = \frac{|G_p|^2}{|S \cap T|},$$

and so $|S \cap T| > 1$.

Since $\mathbf{O}_p(G) = 1$ and $\mathbf{J}(P) > 1$ for $P \in \text{Syl}_p(G)$, the Thompson subgroups of the Sylow p -subgroups of G cannot all be equal, so we can choose $S, T \in \text{Syl}_p(G)$ with $\mathbf{J}(S) \neq \mathbf{J}(T)$. Do this so that $D = S \cap T$ is as large as possible, and observe that $D < S$ since $S \neq T$. By the computation of the first paragraph, $D > 1$, and hence $\mathbf{N}_G(D) < G$, and we can choose a maximal subgroup $M \supseteq \mathbf{N}_G(D)$. Now $\mathbf{N}_G(D)$ contains a p -central element by Step 5, and thus by Step 5 with p and q reversed, M cannot be of q -type. Then M is of p -type, and so by Step 8, the Sylow p -subgroups of M are full Sylow p -subgroups of G .

Choose $U \in \text{Syl}_p(M)$ with $U \supseteq M \cap S$, and observe that

$$U \cap S = U \cap M \cap S = M \cap S \supseteq \mathbf{N}_S(D) > D.$$

Since $U \in \text{Syl}_p(G)$, it follows by the maximality of $|D|$ that $\mathbf{J}(S) = \mathbf{J}(U)$, and similarly, we can choose $V \in \text{Syl}_p(M)$ such that $\mathbf{J}(V) = \mathbf{J}(T)$. Now $\mathbf{J}(U)$ and $\mathbf{J}(V)$ are conjugate in M since the Sylow subgroups U and V are conjugate. By Step 8, however, $\mathbf{J}(U) \triangleleft M$, and we deduce that $\mathbf{J}(S) = \mathbf{J}(U) = \mathbf{J}(V) = \mathbf{J}(T)$. This contradicts the choice of S and T , and the proof is complete. ■

Permutation Groups

8A

In this chapter, we return to the study of group actions on abstract sets. Let G act on a nonempty finite set Ω , and recall that such an action defines a natural homomorphism (the permutation representation associated with the action) from G into the symmetric group $\text{Sym}(\Omega)$. We say that G is a **permutation group** on Ω if the action is faithful, or equivalently, if the permutation representation is an injective homomorphism. If G is a permutation group on Ω , it is common to identify G with its isomorphic copy in $\text{Sym}(\Omega)$, so one can view permutation groups on Ω simply as subgroups of $\text{Sym}(\Omega)$.

Of course, if we intend to use a permutation representation of G to make statements about the group G itself, it is essential that the corresponding action should be faithful, but for many purposes, and, in particular, for the basic definitions of the subject, faithfulness is irrelevant. For that reason, and despite the title of this chapter, we will generally not assume that our actions are faithful except when such an assumption is really necessary. We will always assume in this chapter, however, that the sets being acted on are finite, although much of the theory works more generally.

Recall that if G acts on Ω , then Ω is partitioned into G -orbits, and that the action is transitive if there is just one orbit: Ω itself. Equivalently, the action of G on Ω is transitive if for every choice of points $\alpha, \beta \in \Omega$, there exists an element $g \in G$ such that $\alpha \cdot g = \beta$.

The following describes the (necessarily nonempty) set of all elements of G that carry α to β in a transitive action. (It is essentially a restatement of Theorem 1.4, which underlies the fundamental counting principle.)

8.1. Lemma. *Suppose that a group G acts transitively on Ω . Fix a point $\alpha \in \Omega$, and let $H = G_\alpha$ be the stabilizer of α in G . For an arbitrary point $\beta \in \Omega$, let $\pi(\beta) = \{x \in G \mid \alpha \cdot x = \beta\}$. Then $\pi(\beta)$ is a right coset of H in G , and π is a bijection from Ω onto the set $\Lambda = \{Hx \mid x \in G\}$ of all right cosets of H .*

Proof. Given $\beta \in \Omega$, choose $g \in G$ such that $\alpha \cdot g = \beta$, and observe that since the elements of H stabilize α , every element of the coset Hg carries α to β , and hence $Hg \subseteq \pi(\beta)$. Conversely, if $x \in \pi(\beta)$, then $\alpha \cdot x = \beta$, and so $\alpha \cdot (xg^{-1}) = \alpha$. Then, $xg^{-1} \in H$, and hence $x \in Hg$, and it follows that $\pi(\beta) = Hg \in \Lambda$.

The map π is injective since if $\pi(\beta) = \pi(\gamma)$, then an element of this set carries α to β and also to γ , and thus $\beta = \gamma$. Finally, π is surjective since for each coset $Hg \in \Lambda$, we have $Hg = \pi(\alpha \cdot g)$. ■

Of course, if G is an arbitrary finite group and $H \subseteq G$ is any subgroup, then G acts transitively on the right cosets of H in G . In the situation of Lemma 8.1, therefore, G acts on Λ , and it is interesting to compare this action with the given action of G on Ω . In fact, the bijection $\pi : \Omega \rightarrow \Lambda$ of Lemma 8.1 is a **permutation isomorphism**, which means that $\pi(\beta \cdot g) = \pi(\beta) \cdot g$ for all $\beta \in \Omega$ and $g \in G$. (The “dot” on the right of this equation, of course, denotes the right multiplication action of G on right cosets of H .) To check that the right cosets of H on each side of the equation $\pi(\beta \cdot g) = \pi(\beta) \cdot g$ are the same, it suffices to observe that each of them contains xg , where $x \in G$ is an arbitrary element that carries α to β .

It should now be apparent that the study of the transitive actions of a group is equivalent to the study of the actions of the group on the sets of right cosets of its various subgroups. Furthermore, we know that the kernel of the action of G on the set of right cosets of a subgroup H is exactly $\text{core}_G(H)$, and thus the study of transitive permutation groups (that is, faithful transitive actions) is equivalent to the study of subgroups having trivial core. In other words, much of permutation-group theory can be subsumed within “pure” group theory. Nevertheless, the permutation point of view provides useful insights and suggests interesting theorems, and that is why we study it. Also, one should remember that historically, permutation groups (as subgroups of symmetric groups) appeared before Cayley gave the modern axiomatic definition of an abstract group. For many years, the permutation group point of view was the only one available in group theory.

Recall that if G acts on Ω and $g \in G$ and $\alpha \in \Omega$, then $(G_\alpha)^g = G_{\alpha \cdot g}$. In a transitive action, therefore, the point stabilizers are all conjugate, and, in particular, if some point stabilizer is trivial, then all of them are trivial.

If the point stabilizers in a transitive action of G on Ω are trivial, it follows by Lemma 8.1 that for each choice of $\alpha, \beta \in \Omega$, there is exactly one element of G that carries α to β . In this situation, where for all α and β , there is a unique element $g \in G$ such that $\alpha \cdot g = \beta$, we say that G is **regular** or **sharply transitive** on Ω . (Conversely, of course, if G is regular on Ω , then there is a unique group element that carries α to α , and so the point stabilizer G_α is the trivial subgroup.) Note that regular actions are automatically faithful.

By the fundamental counting principle, we see that if G is transitive on Ω , then $|G|$ is a multiple of $|\Omega|$. (The integer $|\Omega|$ is the **degree** of the action.) In particular, $|G| \geq |\Omega|$, and G is regular if and only if equality holds. We mention that a not-necessarily-transitive action in which all point stabilizers are trivial is said to be **semiregular**.

The notion of transitivity can also be refined in a different direction. Suppose that G acts on a set Ω containing at least k points, where k is some positive integer, and consider the set $\mathcal{O}_k(\Omega)$ of ordered k -tuples $(\alpha_1, \alpha_2, \dots, \alpha_k)$ of distinct points $\alpha_i \in \Omega$. (The condition $|\Omega| \geq k$ is needed so that $\mathcal{O}_k(\Omega)$ will be nonempty.) The action of G on Ω defines a natural componentwise action of G on $\mathcal{O}_k(\Omega)$ via the formula

$$(\alpha_1, \alpha_2, \dots, \alpha_k) \cdot g = ((\alpha_1) \cdot g, (\alpha_2) \cdot g, \dots, (\alpha_k) \cdot g).$$

(It is a triviality that this is a genuine group action.) We say that G is **k -transitive** on Ω if the associated componentwise action of G on $\mathcal{O}_k(\Omega)$ is transitive. Equivalently, and continuing to assume that $|\Omega| \geq k$, an action of G on Ω is k -transitive if given any two ordered k -tuples $(\alpha_1, \alpha_2, \dots, \alpha_k)$ and $(\beta_1, \beta_2, \dots, \beta_k)$ of distinct points of Ω , there exists an element $g \in G$ such that $(\alpha_i) \cdot g = \beta_i$ for $1 \leq i \leq k$. (Note that although we require that the α_i are distinct and that the β_i are distinct, there is no requirement that the sets $\{\alpha_i\}$ and $\{\beta_i\}$ should be disjoint.)

Observe that if G is k -transitive on Ω , then G is automatically m -transitive for all integers m with $1 \leq m \leq k$. In particular, a k -transitive action is necessarily 1-transitive, which simply means that it is transitive, and thus in general, k -transitivity is stronger than transitivity. An action that is k -transitive with $k > 1$ is said to be **multiply transitive**, and if $k = 2$, the action is **doubly transitive**. In particular, multiply transitive actions are always doubly transitive.

If $|\Omega| = n$, it is easy to see that $|\mathcal{O}_k(\Omega)| = n(n-1) \cdots (n-k+1)$, where there are exactly k factors in the product. If G is k -transitive on Ω , therefore, then because it is transitive on $\mathcal{O}_k(\Omega)$, the fundamental counting principle guarantees that $|G|$ must be a multiple of $|\mathcal{O}_k(\Omega)|$. In particular, if G is doubly transitive of degree n , then $n(n-1)$ must divide $|G|$.

What are some examples of multiply transitive group actions? First, it is easy to see that the full symmetric group S_n is n -transitive on $\Omega = \{1, 2, \dots, n\}$. In fact, given two ordered n -tuples (α_i) and (β_i) of distinct points of Ω , there is obviously a unique element $g \in S_n$ that carries α_i to β_i for all i . In general, if an action is k -transitive, and if for each pair of k -tuples of distinct points there is a unique element of G carrying one to the other, we say that the action is **sharply k -transitive**. In other words, G is sharply k -transitive on Ω precisely when it is sharply transitive (i.e., regular) on the set $\mathcal{O}_k(\Omega)$. In particular, if G is sharply k -transitive on Ω , where $|\Omega| = n$, then $|G| = |\mathcal{O}_k(\Omega)| = n(n-1)(n-2) \cdots (n-k+1)$.

The alternating group A_n is $(n-2)$ -transitive on $\Omega = \{1, 2, \dots, n\}$. To see this, observe that the stabilizer of the $(n-2)$ -tuple $t = (1, 2, \dots, n-2)$ in the symmetric group S_n contains only the identity and the transposition exchanging the points $n-1$ and n . The stabilizer of t in A_n , therefore, is trivial, and so by the fundamental counting principle, the A_n -orbit of t has cardinality equal to $|A_n|$. But $|A_n| = n!/2 = |\mathcal{O}_{n-2}(\Omega)|$, and it follows that A_n is transitive on $\mathcal{O}_{n-2}(\Omega)$ as wanted. In fact, since a point stabilizer in the action of A_n on $\mathcal{O}_{n-2}(\Omega)$ is trivial, A_n is sharply transitive on this set of $(n-2)$ -tuples, and so A_n is sharply $(n-2)$ -transitive on Ω .

We mention that A_n and S_n are the only subgroups of S_n that are $(n-2)$ -transitive on $\Omega = \{1, \dots, n\}$. One way to see this is to observe that if $G \subseteq S_n$ is $(n-2)$ -transitive, then $|\mathcal{O}_{n-2}(\Omega)| = n!/2$ must divide $|G|$, and thus G has index at most 2 in S_n . It follows that G contains every element of order 3 in S_n , and, in particular, it contains all 3-cycles. It is not hard to see, however, that the 3-cycles in S_n generate A_n , and thus $A_n \subseteq G$. In other words, G is A_n or S_n , as claimed.

We have seen that S_n and A_n are respectively sharply n -transitive and $(n-2)$ -transitive of degree n . In fact, unless k is tiny, there are only a few other examples (sharp or not) of k -transitive permutation groups. One of these is the Mathieu group M_{12} , which is one of the 26 sporadic simple groups. It is sharply 5-transitive on 12-points, and so

$$|M_{12}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95,040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11.$$

The stabilizer of a point in M_{12} is the sporadic simple group M_{11} , which is sharply 4-transitive on the remaining 11 points. (In general, we will see that if $k > 1$, then a point stabilizer in a k -transitive action on n points necessarily acts $(k-1)$ -transitively on the remaining $n-1$ points, and it is easy to check that sharpness is inherited in this situation.) Of course M_{11} has index 12 in M_{12} , and so

$$|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7,920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11.$$

In fact, M_{11} is the smallest of the sporadic simple groups. A point stabilizer in M_{11} is sharply 3-transitive on the remaining 10 points, but it is not simple. This group, which is sometimes called M_{10} , has order $7920/11 = 720$. It has a normal subgroup of index 2, isomorphic to the alternating group A_6 , but M_{10} is *not* isomorphic to S_6 . In fact, there are three nonisomorphic groups of order 720 that contain copies of A_6 ; these are S_6 , M_{10} and $PGL(2, 9)$. (Recall that $PGL(n, q)$ is the projective general linear group; it is the factor group $GL(n, q)/Z$, where $Z = Z(GL(n, q))$ is the group of scalar matrices in $GL(n, q)$.) Each of these three groups of order 720 happens to be a permutation group of degree 10. Both M_{10} and $PGL(2, 9)$ are 3-transitive in their 10-point actions, but S_6 is only 2-transitive and not 3-transitive. (One way to distinguish these three groups is via their Sylow 2-subgroups: a Sylow 2-subgroup of S_6 is a direct product of D_8 with a cyclic group of order 2; a Sylow 2-subgroup of $PGL(2, 9)$ is D_{16} and a Sylow 2-subgroup of M_{10} is the semidihedral group SD_{16} .)

The Mathieu group M_{24} (which is another of the 26 sporadic simple groups) is 5-transitive on 24-points. But it is not sharply 5-transitive; the stabilizer in M_{24} of a 5-tuple of distinct points has order 48. It follows that

$$|M_{24}| = 48|O_5| = 48 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 = 244, 823, 040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23.$$

The stabilizer of a point in M_{24} is the Mathieu group M_{23} , which is also one of the sporadic simple groups; it is 4-transitive on the remaining 23 points. Clearly, M_{23} has index 24 in M_{24} , and so $|M_{23}| = 10, 200, 960$. The stabilizer of a point in M_{23} is the simple Mathieu group M_{22} , which is 3-transitive on the remaining 22 points and has order 443, 520. The stabilizer of a point in M_{22} is simple, but it is not one of the sporadic simple groups; it is isomorphic to $PSL(3, 4)$. (As a consequence of Lemma 8.29, we shall see that $PSL(3, 4)$ is a 2-transitive permutation group of degree 21.)

For $k \geq 4$, we have named four k -transitive permutation groups other than S_n and A_n in their natural actions. These four groups are M_{24} and M_{12} , which are 5-transitive, and M_{23} and M_{11} , which are 4-transitive. In fact, there are no other examples. The only known proofs of this, however, require an appeal to the classification of simple groups. (But there is an elementary argument due to C. Jordan that shows that a *sharply* k -transitive group with $k \geq 4$ must either be a full symmetric or alternating group, or else k is 4 or 5 and the degree is 11 or 12, respectively.) We shall see, however, that there are infinitely many 3-transitive permutation groups other than symmetric and alternating groups, and in fact there are infinitely many *sharply* 3-transitive groups. (See Problem 8A.17.)

8.2. Lemma. *Suppose that a group G acts transitively on Ω . Let $\gamma \in \Omega$, and fix an integer $k \leq |\Omega|$. Then G is k -transitive on Ω if and only if the point stabilizer G_γ is $(k - 1)$ -transitive on $\Omega - \{\gamma\}$.*

Proof. First, assume that G is k -transitive on Ω . Let

$$a = (\alpha_1, \alpha_2, \dots, \alpha_{k-1}) \quad \text{and} \quad b = (\beta_1, \beta_2, \dots, \beta_{k-1})$$

be $(k-1)$ -tuples of distinct points of $\Omega - \{\gamma\}$, and let A and B be the k -tuples constructed by appending γ to a and b , respectively. The entries in a and in b are distinct and lie in $\Omega - \{\gamma\}$, and hence the entries in each of A and B are distinct. But G is k -transitive on Ω , so there exists an element $g \in G$ that carries A to B . Then g carries a to b and γ to γ , or, in other words, $a \cdot g = b$ and $g \in G_\gamma$. It follows that G_γ is $(k-1)$ -transitive on $\Omega - \{\gamma\}$, as wanted.

Conversely, suppose that G_γ is $(k-1)$ -transitive on $\Omega - \{\gamma\}$, and let

$$A = (\alpha_1, \alpha_2, \dots, \alpha_k) \quad \text{and} \quad B = (\beta_1, \beta_2, \dots, \beta_k)$$

be ordered k -tuples of distinct points of Ω . Since the action of G on Ω is transitive, we can choose elements $x, y \in G$ such that $(\alpha_k) \cdot x = \gamma$ and $(\beta_k) \cdot y = \gamma$. Then $A \cdot x$ and $B \cdot y$ are k -tuples of distinct points of Ω , and the last entry of each of them is γ .

Let a and b be the $(k-1)$ -tuples obtained from $A \cdot x$ and $B \cdot y$, respectively, by deleting the last entry. The entries of each of a and b , therefore, are distinct and lie in $\Omega - \{\gamma\}$, and thus there exists an element $g \in G_\gamma$ that carries a to b . Since $A \cdot x$ and $B \cdot y$ can be obtained from a and b by appending γ , which is fixed by g , we see that $(A \cdot x) \cdot g = B \cdot y$, and thus xgy^{-1} is an element of G that carries A to B . This completes the proof. ■

We will use Lemma 8.2 to construct an infinite family of 3-transitive permutation groups, but we start with a family of 2-transitive group actions. Recall that if $n \geq 1$ and q is a prime power, then the general linear group $GL(n, q)$ is the group of invertible $n \times n$ matrices over the field F of order q , and the subgroup $SL(n, q)$, the special linear group, is the set of determinant-one matrices in $GL(n, q)$.

Since $GL(n, q)$ is isomorphic to the group of invertible linear transformations of an n -dimensional vector space V over F , it is customary to identify the matrix group $GL(n, q)$ with the corresponding group of linear transformations. One often speaks, therefore, of the “natural action” of $GL(n, q)$ on V , and the “natural action” of its subgroup $SL(n, q)$ on V . But, of course, we should remember that the isomorphism between $GL(n, q)$ and the group of linear transformations of V is not really natural; it depends on the choice of a basis for V .

8.3. Lemma. *Let V be an n -dimensional vector space over a field F of order q , where $n \geq 2$. Then for every prime-power q , the natural action of $SL(n, q)$ on the set of all one-dimensional subspaces of V is doubly transitive.*

Proof. First, observe that invertible linear transformations of V carry subspaces to subspaces and preserve dimensions, and thus $SL(n, q)$ actually does permute the set of one-dimensional subspaces of V . Also, since $n \geq 2$, there are at least two of these, and so it makes sense to ask if the action is 2-transitive.

Now let $a_1, a_2, b_1, b_2 \in V$ be nonzero, and consider the one-dimensional subspaces Fa_1, Fa_2, Fb_1 and Fb_2 . Assuming that $Fa_1 \neq Fa_2$ and that $Fb_1 \neq Fb_2$, we must show that there exists an element $g \in SL(n, q)$ that carries Fa_1 to Fb_1 and Fa_2 to Fb_2 . Since $Fa_1 \neq Fa_2$, the vectors a_1 and a_2 are linearly independent, and so there exist vectors a_3, a_4, \dots, a_n such that $\{a_i \mid 1 \leq i \leq n\}$ is a basis for V , and similarly, we can expand the set $\{b_1, b_2\}$ to a basis $\{b_i \mid 1 \leq i \leq n\}$.

Since the a_i form a basis, there is some (unique) linear transformation t on V that maps a_i to b_i for $1 \leq i \leq n$, and since the b_i form a basis, t must be invertible. Thus $t \in GL(n, q)$, and t carries Fa_1 to Fb_1 and Fa_2 to Fb_2 . The proof is not yet complete, however, because t may not have determinant 1.

Let $\delta = \det(t)$, so that $0 \neq \delta \in F$, and let $\epsilon = \delta^{-1}$. Now $\{\epsilon b_1, b_2, \dots, b_n\}$ is a basis for V , and so, reasoning as before, there is a unique invertible linear transformation x on V that carries b_1 to ϵb_1 and b_i to b_i for $2 \leq i \leq n$. The matrix corresponding to x with respect to the basis $\{b_i\}$ is diagonal, with $(1, 1)$ -entry equal to ϵ and all other diagonal entries equal to 1. Thus $\det(x) = \epsilon$, and hence $\det(tx) = \det(t)\det(x) = \epsilon\delta = 1$ and $tx \in SL(n, q)$. Now tx carries a_1 to ϵb_1 , and so it carries Fa_1 to Fb_1 . It also carries a_2 to b_2 , and hence it carries Fa_2 to Fb_2 . This completes the proof. ■

Clearly, scalar multiplication by a nonzero field element on a vector space fixes all subspaces. It follows in the situation of Lemma 8.3 that the subgroup Z of $SL(n, q)$ consisting of all determinant-one scalar matrices is contained in the kernel of the action on the set of one-dimensional subspaces of V , and thus the factor group $SL(n, q)/Z = PSL(n, q)$ acts on this set. It is not hard to see that in fact, Z is the full kernel of the action, and hence $PSL(n, q)$ acts faithfully, and so it is a doubly transitive permutation group. We prove this in Lemma 8.29.

8.4. Corollary. *Let $n \geq 2$. Then the group $GL(n, 2)$ is doubly transitive on the set of nonzero vectors in the n -dimensional vector space V over the field of order 2.*

Proof. Since the field has order 2, a one-dimensional subspace of V contains exactly one nonzero vector, and each nonzero vector, of course, lies in exactly one one-dimensional subspace. The action of $GL(n, 2) = SL(n, 2)$ on the

nonzero vectors of V , therefore, is permutation-isomorphic to its action on the one-dimensional subspaces of V , which we know is doubly transitive. ■

Next, we need the following easy result.

8.5. Lemma. *Suppose that a group G acts transitively on Ω , and let $A = G_\alpha$, where $\alpha \in \Omega$. Then a subgroup $N \subseteq G$ is transitive on Ω if and only if $AN = G$, and N is regular on Ω if and only if in addition, $A \cap N = 1$. Also, if N is regular and normal in G , then the conjugation action of A on the nonidentity elements of N is permutation isomorphic to the action of A on the set $\Omega - \{\alpha\}$.*

Proof. First, $AN = G$, if and only if every right coset of A in G has the form An for some element $n \in N$, and this happens if and only if N acts transitively by right multiplication on the right cosets of A in G . The right multiplication action of G on these cosets, however, is permutation isomorphic to the action of G on Ω , and so N is transitive on the right cosets of A if and only if it is transitive on Ω . This shows that as claimed, N is transitive on Ω if and only if $AN = G$. Also, assuming that N is transitive, we know that it is regular if and only if the point stabilizer $N_\alpha = A \cap N$ is trivial.

Now suppose that N is regular and normal, and let $\pi : N \rightarrow \Omega$ be the map defined by $\pi(n) = \alpha \cdot n$ for $n \in N$. To show that π is injective, let $x, y \in N$, and suppose $\pi(x) = \pi(y)$. Then $\alpha \cdot x = \alpha \cdot y$, and thus $x = y$ since by regularity, x is the unique element of N that carries α to $\alpha \cdot x$. For surjectivity, observe that since N is transitive, every element of Ω has the form $\alpha \cdot n = \pi(n)$ for some element $n \in N$. Thus π is a bijection from N to Ω , and since $\pi(1) = \alpha$, it follows that π defines a bijection from $N - \{1\}$ onto $\Omega - \{\alpha\}$. To show that this is a permutation isomorphism of the actions of A on these two sets, we must check that $\pi(n^a) = \pi(n) \cdot a$ for $a \in A$ and nonidentity elements $n \in N$. We have

$$\pi(n^a) = \alpha \cdot (a^{-1}na) = (\alpha \cdot n) \cdot a = \pi(n) \cdot a,$$

as required, where the second equality holds because $a \in A = G_\alpha$. ■

8.6. Corollary. *Let A be a group that acts via automorphisms on a finite group N , and assume that the resulting action of A on the set of nonidentity elements of N is k -transitive for some positive integer k . Let $G = N \rtimes A$, and view N and A as subgroups of G . Then the right-multiplication action of G on the set of right cosets of A in G is $(k+1)$ -transitive.*

Proof. Let Ω be the set of right cosets of A in G , and observe that $A = G_\alpha$, where $\alpha \in \Omega$ is the point $\alpha = A$. Since G is certainly transitive on Ω , it suffices by Lemma 8.2 to show that A is k -transitive on $\Omega - \{\alpha\}$. But

$AN = G$ and $A \cap N = 1$, and hence N is a regular normal subgroup of G by Lemma 8.5. Also by Lemma 8.5, the action of A on $\Omega - \{\alpha\}$ is permutation isomorphic to its action on $N - \{1\}$, and by hypothesis, this latter action is k -transitive. This completes the proof. ■

Finally, we can construct the promised family of 3-transitive permutation groups.

8.7. Corollary. *Let V be an elementary abelian 2-group of order 2^n with $n \geq 2$, and write $G = V \rtimes GL(n, 2)$, where the action of $GL(n, 2)$ is defined by identifying V with a vector space of dimension n over a field of order 2. Then G is a 3-transitive permutation group of degree 2^n .*

Proof. Write $A = GL(n, 2)$. By Corollary 8.4, the action of A on the nonidentity elements of V is 2-transitive, and hence by Corollary 8.6, the action of G on the right cosets of A is 3-transitive. The degree of this action is $|G : A| = |V| = 2^n$, and so all that remains is to show that the action of G on the right cosets of A is faithful. The kernel K of the action, however, is normal in G , and since $K \subseteq A$, we have $V \cap K = 1$, and so $K \subseteq \mathbf{C}_G(V)$. Then K acts trivially on V , and since the natural action of $A = GL(n, 2)$ on V is faithful, it follows that $K = 1$. ■

Actually, Corollary 8.6 is less general than it may appear to be. In fact, the integer k in the statement of that result can almost never exceed 2.

8.8. Lemma. *Let A be a group that acts via automorphisms on a finite group N , and suppose that the resulting action of A on the nonidentity elements of N is k -transitive, with $k \geq 1$. Then*

- (a) N is an elementary abelian p -group for some prime p .
- (b) If $k > 1$ then either $p = 2$ or $|N| = 3$.
- (c) If $k > 2$, then $|N| = 4$ and $k = 3$.

Proof. Let $x \in N$ have prime order p . Since A acts via automorphisms and is transitive on the nonidentity elements of N , it follows that every nonidentity element of N has order p , and hence N is a p -group. Then $\mathbf{Z}(N)$ is nontrivial, and so we can assume that x is central in N , and hence every nonidentity element of N is central. Thus N is abelian, proving (a).

Now assume that the action of A on the nonidentity elements of N is 2-transitive. If $p > 2$ then x and x^{-1} are distinct nonidentity elements, and if $|N| > 3$, we can choose a nonidentity element y of N different from both x and x^{-1} . By 2-transitivity, there is an element $a \in A$ that carries the ordered pair (x, x^{-1}) to the ordered pair (x, y) . Then $x = x^a$ and $y = (x^{-1})^a = (x^a)^{-1} = x^{-1}$. This contradiction proves (b).

Finally, assume that the action is 3-transitive. In particular, $3 \leq k \leq |N - \{1\}|$, so $|N| \geq 4$, and we have $p = 2$ by (b). Choose a nonidentity element y of N different from x , and observe that $xy \neq 1$ and that xy is different from both x and y . If $|N| > 4$, choose a nonidentity element z different from x , y and xy , and consider the ordered triples (x, y, xy) and (x, y, z) , which consist of distinct elements. By 3-transitivity, there exists $a \in A$ such that $x = x^a$, $y = y^a$ and $z = (xy)^a = x^a y^a = xy$, which is a contradiction. Thus $|N| = 4$, and so $k \leq |N - \{1\}| = 3$. ■

We close this section with a variation on Lemma 8.8(a). In order to conclude that N is an elementary abelian p -group in that lemma, we shall see that the assumption that A acts transitively on the set of nonidentity elements of N is unnecessarily strong.

We say that an action of G on Ω is **half-transitive** if all orbits have equal size. (A transitive action, therefore, is certainly half-transitive.) The following is a result of D. S. Passman and the author.

8.9. Theorem. *Let A be a finite group that acts faithfully via automorphisms on a finite group N , and assume that the resulting action of A on the nonidentity elements of N is half-transitive. Then either the action is Frobenius, or else N is an elementary abelian p -group for some prime p , and no nonidentity proper subgroup of N admits the action of A .*

Note that a Frobenius action of A on N is automatically half-transitive on the nonidentity elements of N because all A -orbits on this set have equal size $|A|$.

We need a preliminary result about finite groups partitioned by normal subgroups.

8.10. Lemma. *Let G be a finite group and let Π be a collection of proper normal subgroups of G . Suppose that $G = \bigcup \Pi$ and that distinct members of Π intersect trivially. Then G is an elementary abelian p -group for some prime p .*

Proof. Let $X \in \Pi$, and observe that if $X \neq Y \in \Pi$, then $X \cap Y = 1$, and so $Y \subseteq \mathbf{C}_G(X)$. It follows that

$$G = X \cup \bigcup_{\substack{Y \in \Pi \\ Y \neq X}} Y \subseteq X \cup \mathbf{C}_G(X).$$

But G cannot be the union of two proper subgroups, and since X is proper, it follows that $\mathbf{C}_G(X) = G$, and hence $X \subseteq \mathbf{Z}(G)$. Since $\bigcup \Pi = G$ and every member of Π is central, we have $\mathbf{Z}(G) = G$, and thus G is abelian.

If $x, y \in G$ have different orders, we argue that they lie in a common member of Π . To see this, assume that $o(x) > o(y)$. Then

$$(xy)^{o(y)} = x^{o(y)}y^{o(y)} = x^{o(y)} \neq 1,$$

where the first equality is valid because G is abelian and the inequality holds because $o(y) < o(x)$. Now let $X, Z \in \Pi$, with $x \in X$ and $xy \in Z$. Then $x^{o(y)} = (xy)^{o(y)}$ is a nonidentity element in $X \cap Z$, and thus $X = Z$. It follows that $xy \in X$, and so $y \in X$, as claimed.

Let $x \in G$ have prime order p , and let $X \in \Pi$ with $x \in X$. We complete the proof now by showing that every nonidentity element $y \in G$ has order p . If $y \in G - X$, then x and y do not lie in a common member of Π , and so $o(y) = o(x) = p$, as wanted. If, on the other hand, y is a nonidentity element of X , choose $z \in G - X$. Then z does not share a member of Π with either x or y , and thus $o(y) = o(z) = o(x) = p$. ■

Proof of Theorem 8.9. For nonidentity elements $x \in N$, write $G_x = \mathbf{C}_N(\mathbf{C}_A(x))$, and let $\Pi = \{C_x \mid 1 \neq x \in N\}$ be the collection of subgroups of N constructed in this way. It is clear that $x \in C_x$, and it follows that $\bigcup \Pi = N$. If $1 \neq y \in C_x$, we argue that $G_y = C_x$. To see this, observe that $\mathbf{C}_A(x)$ centralizes y , and thus $\mathbf{C}_A(x) \subseteq \mathbf{C}_A(y)$. But $\mathbf{C}_A(x)$ and $\mathbf{C}_A(y)$ are subgroups of index r in A , where r is the common size of the A -orbits on $N - \{1\}$, and thus equality holds, and $\mathbf{C}_A(x) = \mathbf{C}_A(y)$. Then

$$C_y = \mathbf{C}_N(\mathbf{C}_A(y)) = \mathbf{C}_N(\mathbf{C}_A(x)) = C_x,$$

as claimed. In particular, this shows that distinct members of the set Π intersect trivially.

Now assume that the action of A on N is not Frobenius, so that $r < |A|$. Then $\mathbf{C}_A(x) > 1$ for nonidentity elements $x \in N$, and since the action of A on N is faithful, $\mathbf{C}_A(x)$ does not act trivially on N . In other words, $C_x < N$, and so Π consists of proper subgroups of N .

We work now to show that the members of Π are normal in N so that we can apply Lemma 8.10. First, observe that r divides $|N| - 1$, and thus r and $|N|$ are coprime. Let $\{x_1, x_2, \dots, x_r\}$ be an A -orbit of nonidentity elements of N , and let K_i be the conjugacy class of x_i in N . (Note that perhaps the classes K_i are not all distinct.)

Since A acts via automorphisms on N and A permutes the elements x_i transitively, it follows that A permutes the set of conjugacy classes K_i transitively. In particular, these classes have equal cardinality, say k , where k is a divisor of $|N|$, and hence k is relatively prime to r .

Now write

$$U = \bigcup_{i=1}^r K_i,$$

and recall that $|K_i| = k$ for all i . Since the sets K_i are conjugacy classes of N , distinct K_i are disjoint, and it follows that $|U|$ is a multiple of k . Furthermore, since the sets K_i are permuted by A , their union U is an A -invariant subset of N . Also, U consists of nonidentity elements, and so it is a union of A -orbits of size r , and we deduce that r divides $|U|$. Now k and r are coprime integers and both divide $|U|$, and it follows that rk divides $|U|$, and in particular, $rk \leq |U|$. But U is the union of the sets K_i for $1 \leq i \leq r$, and each of these sets has cardinality k , and thus $|U| \leq rk$. Thus $|U| = rk$, and so the sets K_i must all be different. This shows that a nonidentity class of N cannot contain distinct members of an A -orbit.

We argue next that every nonidentity conjugacy class of N is contained in one of the subgroups C_x in Π . Since distinct members of Π intersect trivially, this will show that each member of Π is a union of classes of N , and thus is normal in N , as wanted. Given a nonidentity class K of N , let $x \in K$. Since A permutes the classes of N and $C_A(x)$ fixes x , it follows that $C_A(x)$ stabilizes the class K , and thus $C_A(x)$ permutes the elements of K . We know, however, that distinct members of K cannot lie in a common A -orbit, and this shows that, in fact, $C_A(x)$ fixes every member of K . Thus $K \subseteq C_N(C_A(x)) = C_x$, as claimed, and hence we can apply Lemma 8.10 to conclude that N is an elementary abelian p -group for some prime p .

Finally, if H is a proper A -invariant subgroup of N , we work to show that $H = 1$. Let $\{x_i, x_2, \dots, x_r\}$ be an A -orbit outside of H , and observe that A permutes the set of cosets Hx_i , and so the set

$$V = \bigcup_{i=1}^r Hx_i$$

is A -invariant. Since $V \subseteq G - H$, it consists of nonidentity elements, and so it is a union of A -orbits of size r . Thus r divides $|V|$, and also, since V is a union of cosets of H , we see that $|H|$ divides $|V|$. By coprimeness, $r|H|$ divides $|V|$, and so $|V| \geq r|H|$, and it follows that the cosets Hx_i are distinct. This shows that no right coset of H other than H can contain distinct elements of an A -orbit.

If $H > 1$, then H can be contained in at most one member of Π . We will show that, in fact, H is contained in some member $C \in \Pi$, and that C also contains every element $x \in N - H$. It follows that $C = N$, which is a contradiction, and this will prove that $H = 1$, as wanted. It suffices, therefore, to show that if $x \in N - H$, then $H \subseteq C_x$.

Since A permutes the right cosets of H , it follows that $C_A(x)$ stabilizes Hx , and so $C_A(x)$ permutes the elements of Hx . But Hx cannot contain distinct elements of an A -orbit, and thus $C_A(x)$ fixes every element of Hx .

We deduce that $Hx \subseteq C_x$, and since C_x is a subgroup that contains x , we conclude that $H \subseteq C_x$. As we have seen, this completes the proof. ■

Note that in the exceptional case of Theorem 8.9, where the action of A on N is Frobenius, we can conclude that N is nilpotent by the theorem of Thompson's thesis. Thus, in all cases, if A acts nontrivially on N and half-transitively on the nonidentity elements, then N is nilpotent.

Problems 8A

8A.1. If A and B are nonisomorphic groups with $|A| = |B|$, show that there exists a permutation group G that has regular subgroups isomorphic to each of A and B . Also, decide whether or not a permutation group can have nonisomorphic regular *normal* subgroups.

Hint. For the first part, take G to be an appropriate symmetric group.

8A.2. Let H be a transitive subgroup of some permutation group G . Show that $C_G(H)$ is semiregular. Deduce that an abelian transitive permutation group must be regular.

8A.3. Given a finite group G with $Z(G) = 1$, show that there exists a permutation group that has two distinct regular normal subgroups, each isomorphic to G .

8A.4. Suppose that U and V are regular normal subgroups of some permutation group G . If $U \cap V = 1$, show that U and V are isomorphic and have trivial centers.

Hint. It is no loss to assume $G = UV$.

8A.5. Let G act k -transitively on some set Ω , and let $H = G_\alpha$, where $\alpha \in \Omega$. Let Δ be the set of points in Ω that are fixed by H . Show that $N_G(H)$ acts r -transitively on Δ , where r is the minimum of k and $|\Delta|$.

8A.6. Let G act transitively on Ω , and let $H = G_\alpha$, where $\alpha \in \Omega$. Let $P \in \text{Syl}_p(H)$, and let Δ be the set of points in Ω that are fixed by P . Show that $N_G(P)$ acts transitively on Δ .

8A.7. Suppose that an abelian group A acts faithfully on a group N , and assume that its action on the nonidentity elements of N is half-transitive. Show that the action is Frobenius, and deduce that A is cyclic.

8A.8. Let G act transitively on Ω , and suppose that $N \triangleleft G$. Show that G permutes the N -orbits in Ω transitively, and deduce that N is half-transitive on Ω .

8A.9. Let G act 2-transitively on Ω , and suppose that $N \triangleleft G$ and that N acts nontrivially. Show that N acts transitively.

Note. In fact, 2-transitivity is more than is really needed here. The right condition is primitivity, which we will discuss in the next section.

8A.10. If G is a solvable 4-transitive permutation group, show that G is isomorphic to the symmetric group S_4 .

Hint. Show that a minimal normal subgroup N of G is regular, and consider the conjugation action of a point stabilizer G_α on N .

Note. In fact, S_4 and S_3 are the only solvable 3-transitive permutation groups, but this is somewhat harder to prove.

8A.11. Show that for every prime power $q > 1$, there exists a solvable sharply 2-transitive permutation group of degree q .

Hint. Consider a field of order q .

8A.12. Let G act transitively on Ω , and let χ be the corresponding permutation character. (Recall that by definition, χ is the function defined by the formula $\chi(g) = |\{\alpha \in \Omega \mid \alpha \cdot g = \alpha\}|$.) Show that G is 2-transitive on Ω if and only if the average value of $\chi(g)^2$ for $g \in G$ is 2.

Hint. Find an action of G whose permutation character is χ^2 , and recall that, in general, the average value of a permutation character is equal to the number of orbits. (See Problem 1A.6 and the note following it.)

8A.13. Let G act 2-transitively on Ω , and let χ be the corresponding permutation character. Find a positive integer m such that G is 3-transitive on Ω if and only if the average value of $\chi(g)^3$ for $g \in G$ is m .

8A.14. Let G act transitively on Ω , and suppose H is a subgroup of G with $|G : H| = m$. Show that H has at most m orbits on Ω , and that if H contains no point stabilizer in G , then H has at most $m/2$ orbits on Ω .

Hint. What is the smallest possible size of an H -orbit?

8A.15. If $H \subseteq G$, we can define an action of $H \times H$ on G by setting $g \cdot (x, y) = x^{-1}gy$ for $g \in G$ and $x, y \in H$. Show that the action of G on the right cosets of H is 2-transitive if and only if $H \times H$ has exactly two orbits on G .

8A.16. Let G be 2-transitive on a set Ω , where $|\Omega| = n$. Suppose that $H \subseteq G$ is transitive, and that $|G : H|$ is relatively prime to $n - 1$. Show that H is 2-transitive.

8A.17. Let q be a power of 2, and let $SL(2, q)$ act on the $q + 1$ one-dimensional subspaces of a two-dimensional vector space over a field of order q . Show that this action is sharply 3-transitive.

8B

Suppose that G acts transitively on Ω , and let $\Delta \subseteq \Omega$ be a nonempty subset. If $g \in G$, we write $\Delta \cdot g = \{\alpha \cdot g \mid \alpha \in \Delta\}$, and we refer to $\Delta \cdot g$ as a **translate** of Δ . The nonempty set Δ is said to be a **block** if every one of its translates other than Δ itself is disjoint from Δ . In other words, Δ is a block if and only if $\Delta \cap \Delta \cdot g = \emptyset$ whenever $g \in G$ and $\Delta \cdot g \neq \Delta$. We stress that we speak of “blocks” only for transitive actions, and that, by definition, blocks are nonempty.

For example, consider the group G of symmetries of square $ABCD$, and view G as a (transitive) permutation group on the vertex set $\Omega = \{A, B, C, D\}$. (Note that $G \cong D_8$, and, in fact, G is a full Sylow 2-subgroup of the symmetric group on Ω .) Now choose a diagonal of the square, say AC , and let $\Delta = \{A, C\}$, the set consisting of the ends of that diagonal. Each symmetry $g \in G$ carries the diagonal AC to a diagonal, and so the only translates of Δ are Δ itself and the set $\{B, D\}$ of endpoints of the other diagonal. In particular, if $\Delta \cdot g \neq \Delta$, then $\Delta \cdot g \cap \Delta$ is empty, and so Δ is a block.

For a more general example, suppose $H \subseteq G$, and let $\Omega = \{Hg \mid g \in G\}$, so that as usual, G acts transitively by right multiplication on Ω . Suppose that $H \subseteq K \subseteq G$, where K is a subgroup, and let $\Delta = \{Hk \mid k \in K\}$. Then Δ is a nonempty subset of Ω , and if $g \in G$, it is easy to see that the translate $\Delta \cdot g$ is exactly the set of those right cosets of H in G that happen to be contained in the coset Kg of K . If $Kg = K$, then $\Delta \cdot g = \Delta$, and if $Kg \neq K$, then $Kg \cap K = \emptyset$, and so no member of $\Delta \cdot g$ can be a member of Δ . We have $\Delta \cdot g \cap \Delta = \emptyset$ in this case, and so Δ is a block.

Of course, in an arbitrary transitive action, the whole set Ω is a block, and so is every one-point subset of Ω . These are referred to as **trivial** blocks, and we say that the given transitive action of G on Ω is **primitive** if the trivial blocks are the only blocks; otherwise, the action is **imprimitive**. Thus, for example, the action of the group of symmetries of a square on the four vertices is imprimitive, and the action of a group G on the right cosets of a subgroup H is imprimitive if there exists a subgroup K such that $H < K < G$. (The condition $H < K$ guarantees that the block $\Delta = \{Hk \mid k \in K\}$ contains more than one point, and the condition $K < G$ guarantees that Δ is not all of Ω .)

8.11. Lemma. *Let G be a group that acts transitively on a set Ω , and suppose that $\Delta \subseteq \Omega$ is a block. Then $|\Delta|$ divides $|\Omega|$ and Δ has exactly $|\Omega|/|\Delta|$ distinct translates. These translates are disjoint blocks; their union is Ω , and they are transitively permuted by G .*

Proof. Let $a, b \in G$, and suppose that $\Delta \cdot a \neq \Delta \cdot b$. Apply b^{-1} to deduce that $\Delta \cdot (ab^{-1}) \neq \Delta$, and thus $\Delta \cdot (ab^{-1}) \cap \Delta = \emptyset$ since Δ is a block. Now apply b to obtain $\Delta \cdot a \cap \Delta \cdot b = \emptyset$. This shows that the distinct translates of Δ are all disjoint, and, in particular, all translates of Δ are blocks. Of course, G permutes the set of translates of Δ transitively.

The union of the distinct translates of Δ is a nonempty G -invariant subset of Ω , and since G is transitive on Ω , this union must be all of Ω . Since the distinct translates of Δ are disjoint, have equal cardinality and cover Ω , there must be exactly $|\Omega|/|\Delta|$ of them, and so this number is an integer. ■

8.12. Corollary. *A transitive group action on a set of prime cardinality is primitive.*

Proof. Let Ω be the relevant set, where $|\Omega|$ is prime. If $\Delta \subseteq \Omega$ is a block, then $|\Delta|$ divides $|\Omega|$, and so $|\Delta| = |\Omega|$ or $|\Delta| = 1$, and hence either $\Delta = \Omega$ or Δ consists of a single point. In either case, Δ is a trivial block, and thus the given action is primitive. ■

The following lemma gives a general, and fairly complete description of the blocks of a transitive action, and it leads to a useful necessary and sufficient condition for primitivity. To state our result, we introduce a bit of notation. If G acts on Ω and $\alpha \in \Omega$, then for each subgroup $K \subseteq G$, we write $\alpha \cdot K = \{\alpha \cdot k \mid k \in K\}$. In other words, $\alpha \cdot K$ is the K -orbit containing the point α .

8.13. Lemma. *Let G be a group that acts transitively on a set Ω , and let $H = G_\alpha$, where $\alpha \in \Omega$. If $K \supseteq H$ is a subgroup, then $\alpha \cdot K$ is a block containing α and $|\alpha \cdot K| = |K : H|$. Also, the map $K \mapsto \alpha \cdot K$ is a bijection from the set of subgroups $\{K \mid H \subseteq K \subseteq G\}$ onto the set of all blocks that contain α .*

Proof. Suppose that $g \in G$ and that the sets $\alpha \cdot K$ and $(\alpha \cdot K) \cdot g$ are not disjoint. We argue that $g \in K$. To see this, observe that there exist elements $x, y \in K$ such that $\alpha \cdot x = (\alpha \cdot y) \cdot g$. Then $ygx^{-1} \in G_\alpha = H \subseteq K$, and since x and y are in K , it follows that $g \in K$, as claimed.

The set $\alpha \cdot K$ is certainly K -invariant, and the result of the previous paragraph shows that K is the full stabilizer of this set in G . Thus $\alpha \cdot K$ uniquely determines K , and it follows that the map $K \mapsto \alpha \cdot K$ is injective

on the set $\{K \mid H \subseteq K \subseteq G\}$. The result of the previous paragraph also shows that the set $\Delta = \alpha \cdot K$ is a block. To see this, observe that if Δ is not disjoint from $\Delta \cdot g$, then $g \in K$, and thus $\Delta \cdot g = \Delta$. Furthermore, the block Δ certainly contains α , and since it is the K -orbit containing α , we have $|\Delta| = |K : H|$ by the fundamental counting principle.

We must now show that given an arbitrary block Δ containing α , there exists a subgroup $K \supseteq H$ such that $\Delta = \alpha \cdot K$. Let K be the stabilizer of Δ in the action of G on subsets of Ω , and observe that $\alpha \cdot K \subseteq \Delta$ since K stabilizes Δ and $\alpha \in \Delta$. To prove the reverse containment, let $\delta \in \Delta$. Since G is transitive on Ω , we can choose $g \in G$ with $\alpha \cdot g = \delta$. Then $\delta \in \Delta \cap \Delta \cdot g$, and thus $\Delta = \Delta \cdot g$ because Δ is a block. Thus $g \in K$, and $\delta = \alpha \cdot g \in \alpha \cdot K$, and this shows that $\Delta = \alpha \cdot K$, as required. Also, we can take $\delta = \alpha$ and $g \in H$ in the above argument, and since we showed that $g \in K$, it follows that $H \subseteq K$. This completes the proof. ■

8.14. Corollary. *Let G be a group that acts transitively on a set Ω containing more than one point, and let $H = G_\alpha$, where $\alpha \in \Omega$. Then G is primitive on Ω if and only if H is a maximal subgroup of G .*

Proof. First, assume that H is maximal. Then by Lemma 8.13, the only blocks that contain α are $\alpha \cdot H = \{\alpha\}$ and $\alpha \cdot G = \Omega$. If Δ is an arbitrary block, then some translate $\Delta \cdot g$ of Δ contains α , and $\Delta \cdot g$ is a block by Lemma 8.11. It follows that $\Delta \cdot g$ is either $\{\alpha\}$ or Ω , and thus Δ is a trivial block. This shows that G is primitive on Ω .

Conversely, if G is primitive, then all blocks containing α are trivial, and thus there are precisely two such blocks: Ω and $\{\alpha\}$. By Lemma 8.13, therefore, there are exactly two subgroups of G that contain H , and thus H is maximal in G . ■

Note that Corollary 8.14 renders Corollary 8.12 superfluous since if $|\Omega|$ is prime, then a point stabilizer has prime index, and hence it is a maximal subgroup. It follows by 8.14 that G is primitive.

The following result gives a useful connection between primitivity and normal subgroups.

8.15. Lemma. *Let G be a group that acts transitively on a set Ω , and let $N \triangleleft G$. Then each orbit of the action of N on Ω is a block for G . In particular, if G is primitive on Ω , then the action of N is either trivial or transitive.*

Proof. Let $g \in G$, and observe that if Δ is an orbit for the action of N , then $\Delta \cdot g$ is an orbit for the action of $N^g = N$. (This is immediate from the fact that if $\alpha \cdot n = \beta$ with $\alpha, \beta \in \Omega$ and $n \in N$, then $(\alpha \cdot g) \cdot (n^g) = \beta \cdot g$.) But distinct N -orbits in Ω are disjoint, and thus if $\Delta \cdot g \neq \Delta$, then $\Delta \cdot g \cap \Delta = \emptyset$.

In other words, Δ is a block for G , as wanted. If G is primitive, it follows that either $\Delta = \Omega$, or else $|\Delta| = 1$. In other words, if N is not transitive on Ω , then all N -orbits have size 1, and thus N acts trivially. ■

An alternative argument for the final assertion of Lemma 8.15 is as follows. If the action of G is primitive and H is a point stabilizer, then H is a maximal subgroup of G by Corollary 8.14. Since $H \subseteq HN \subseteq G$, there are just two possibilities. Either $HN = G$, in which case it is easy to see that N is transitive on Ω , or else $HN = H$. In the latter situation, $N \subseteq H$, and thus N is contained in every conjugate of H , and it follows that N fixes all points in Ω .

Next, we relate primitivity and multiple transitivity.

8.16. Lemma. *Suppose that G is a group with a doubly transitive action on Ω . Then G is primitive on Ω .*

Proof. If G is imprimitive, there exists a nontrivial block Δ , and since Δ does not consist of just one point, we can choose distinct points $\alpha, \beta \in \Delta$. Also, Δ is not all of Ω , and so we can choose $\gamma \in \Omega - \Delta$, and, in particular, $\gamma \neq \alpha$. By 2-transitivity, there exists an element $g \in G$ that carries the pair (α, β) to the pair (α, γ) . In particular, $\alpha \cdot g = \alpha$, and thus $\alpha \in \Delta \cap \Delta \cdot g$. But Δ is a block, and this forces $\Delta \cdot g = \Delta$, and since $\beta \in \Delta$, we have $\beta \cdot g \in \Delta \cdot g = \Delta$. This is a contradiction, however, because $\beta \cdot g = \gamma$ and $\gamma \notin \Delta$. ■

It is easy to find examples of primitive actions that are not 2-transitive. For example, consider the dihedral group D_{2p} of order $2p$, where $p > 3$ is prime. By Corollary 8.12 or Corollary 8.14, this group acts primitively on the p cosets of a subgroup of order 2. But $p - 1$ does not divide $|D_{2p}|$, so the action cannot be 2-transitive. In this context, we mention a remarkable result of W. Burnside that shows that a (necessarily primitive) transitive permutation group of prime degree p must be 2-transitive except possibly when a Sylow p -subgroup is normal. Burnside's proof of this fact was character theoretic, but a comparatively easy non-character proof was found by H. Wielandt. (Wielandt's proof can be found in the book *Permutation Groups* by D. S. Passman.)

As Burnside's theorem on primitive permutation groups of prime degree suggests, once one knows that a group acts primitively on some set, it sometimes does not require a great deal of additional information to deduce that the action is multiply transitive. For example, suppose that G is a primitive permutation group on Ω , and assume that G contains at least one transposition. (Recall that a transposition is a permutation that exchanges two

points and fixes all others. Also, recall the notation (α, β) for the transposition exchanging α with β .) If G is primitive and contains a transposition, a theorem of C. Jordan asserts that G is the full symmetric group on Ω , and so, of course, it is multiply transitive. We will obtain this result as a corollary of a much more general theorem, also due to Jordan, but there is also an entirely elementary and rather geometric proof that we cannot resist presenting first. (We also cannot resist mentioning that we are following in Jordan's footsteps here: he was the author of the very first group-theory book, published in 1870. His *Traité des Substitutions*, of course, deals only with permutation groups since Cayley's modern, abstract point of view was not enunciated until 1878.)

8.17. Theorem (Jordan). *Let G be a primitive permutation group on Ω , and suppose that G contains a transposition. Then G is the full symmetric group on Ω .*

Proof. Since every element of $\text{Sym}(\Omega)$ is a product of transpositions, it suffices to show that G contains all transpositions on Ω . To do this, consider the (undirected) graph with vertex set Ω , in which distinct points α and β are joined by an edge precisely when the transposition (α, β) is an element of G .

If $x = (\alpha, \beta)$ and $g \in G$ is arbitrary, it is easy to see that x^g is the transposition $(\alpha \cdot g, \beta \cdot g)$, which exchanges $\alpha \cdot g$ and $\beta \cdot g$. Of course, if $x \in G$, then also $x^g \in G$, and this shows that if α and β are two points joined by an edge in our graph, then their images under g are also joined by an edge. In other words, the permutations in G define automorphisms of the graph; they carry points to points and edges to edges.

Now consider the connected components of the graph, viewing each component as a nonempty set of vertices. (In other words, no edge joins a point in one component to a point in a different component, and within each component, any two distinct points can be joined by a path consisting of one or more edges.) If Δ is such a component, then since $g \in G$ induces a graph automorphism, it follows that $\Delta \cdot g$ must also be a component. Now if Δ meets $\Delta \cdot g$ nontrivially, then $\Delta \cup \Delta \cdot g$ is a connected set that contains the components Δ and $\Delta \cdot g$. This set, therefore must be equal to each of these components, and thus $\Delta = \Delta \cdot g$. In other words, if Δ and its translate $\Delta \cdot g$ are not disjoint, they cannot be distinct, and hence Δ is a block. The action of G is primitive, however, and hence Δ must be a trivial block, and so either Δ is all of Ω or Δ consists of just one point. By hypothesis, our graph has at least one edge, and so there is a component Δ consisting of more than one point. Then $\Delta = \Omega$, which means that the graph is connected.

Each two points $\alpha, \beta \in \Omega$ are joined by a path, and we define the distance $d(\alpha, \beta)$ to be the length of the shortest path from α to β , where we set $d(\alpha, \alpha) = 0$. Thus $d(\alpha, \beta) = 1$ precisely when $\alpha \neq \beta$ and there is an edge joining α to β . Equivalently, $d(\alpha, \beta) = 1$ if and only if the group G contains the transposition (α, β) . It suffices, therefore, to show that $d(\alpha, \beta) \leq 1$ for all $\alpha, \beta \in \Omega$.

Suppose (for a contradiction) that there exist α and β in Ω with $d = d(\alpha, \beta) > 1$, and choose these points so that $d > 1$ is as small as possible. Since there is a path of length d joining α and β , there must exist a point $\gamma \in \Omega$ such that $d(\alpha, \gamma) = d - 1$ and $d(\gamma, \beta) = 1$. Now $d - 1 \geq 1$, and so by the minimality of d , it follows that $d(\alpha, \gamma) = 1$, and thus the transposition $x = (\alpha, \gamma)$ is an element of G , as is the transposition $y = (\gamma, \beta)$. Then $x^y = (\alpha \cdot y, \gamma \cdot y) = (\alpha, \beta)$, and of course $x^y \in G$. Then α and β are joined by an edge, and this is a contradiction since $d(\alpha, \beta) = d > 1$. ■

To state the more general theorem of Jordan, we introduce some additional notation. If G acts on Ω and $\Lambda \subseteq \Omega$ is an arbitrary subset, we write

$$G_\Lambda = \{g \in G \mid \alpha \cdot g = \alpha \text{ for all } \alpha \in \Lambda\},$$

so that G_Λ is the **pointwise stabilizer** of Λ . This should be distinguished from the **setwise stabilizer**,

$$G_{(\Lambda)} = \{g \in G \mid \Lambda \cdot g = \Lambda\}.$$

Note that $G_{(\Lambda)}$ acts on Λ , and G_Λ is the kernel of this action, so that $G_\Lambda \triangleleft G_{(\Lambda)}$. Also, note that $G_{(\Lambda)} = G_{(\Omega - \Lambda)}$, and thus $G_{\Omega - \Lambda} \triangleleft G_{(\Lambda)}$.

8.18. Theorem (Jordan). *Let G be a group with a primitive action on a set Ω , and let $\Lambda \subseteq \Omega$ with $|\Lambda| \leq |\Omega| - 2$. Suppose that G_Λ acts primitively on $\Omega - \Lambda$. Then the action of G on Ω is $(|\Lambda| + 1)$ -transitive.*

To see that Theorem 8.18 actually does imply Theorem 8.17, suppose that G is a primitive permutation group on Ω , and assume that the transposition (α, β) is an element of G . Take $\Lambda = \Omega - \{\alpha, \beta\}$, so that $|\Lambda| = n - 2$, where $n = |\Omega|$. Since $(\alpha, \beta) \in G_\Lambda$, it follows that G_Λ is transitive on $\{\alpha, \beta\} = \Omega - \Lambda$, and, in fact, this action is primitive since $\Omega - \Lambda$ has prime cardinality 2. By Theorem 8.18, therefore, G is $(n - 1)$ -transitive on Ω , and so

$$|G| \geq |\mathcal{O}_{n-1}(\Omega)| = n \cdot (n - 1) \cdot \cdots \cdot 3 \cdot 2 = n! = |\text{Sym}(\Omega)|.$$

Thus G is the full symmetric group on Ω , as is asserted by Theorem 8.17.

We also have the following closely related result.

8.19. Corollary. *Suppose that G is a primitive permutation group on Ω , and assume that G contains a 3-cycle. Then G is either the full symmetric group or the alternating group on Ω .*

Proof. Suppose that (α, β, γ) is a 3-cycle contained in G , and let $\Lambda = \Omega - \{\alpha, \beta, \gamma\}$. Then G_Λ contains the 3-cycle (α, β, γ) , and hence G_Λ is transitive on $\Omega - \Lambda$, and it is primitive since 3 is prime. Writing $n = |\Omega|$, we have $|\Lambda| + 1 = n - 2$, and it follows by Theorem 8.18 that G is $(n - 2)$ -transitive on Ω . As we have seen, this guarantees that G is either the full symmetric group or the alternating group on Ω . ■

We begin work toward a proof of Theorem 8.18 with the following sufficient condition for primitivity.

8.20. Lemma. *Let G be a group acting transitively on Ω , and let $H \subseteq G$ be a subgroup. Let $X \subseteq \Omega$ be an H -orbit, and assume that H is primitive on X and that $|X| > |\Omega|/2$. Then G is primitive on Ω .*

Proof. Let Δ be a block for the action of G on Ω . We argue that if $\Delta < \Omega$, then $\Delta \cap X$ contains at most one point. To see this, let $h \in H$, and observe that $(\Delta \cap X) \cdot h = \Delta \cdot h \cap X$. If this set is different from $\Delta \cap X$, then clearly $\Delta \cdot h \neq \Delta$, and since Δ is a block for G , it follows that $\Delta \cdot h \cap \Delta = \emptyset$. If $(\Delta \cap X) \cdot h \neq (\Delta \cap X)$, therefore, we have $(\Delta \cap X) \cap (\Delta \cap X) \cdot h = \emptyset$, and so if $\Delta \cap X$ is nonempty, it is a block for the action of H on X . By assumption, however, H is primitive on X , and thus if $\Delta \cap X$ is nonempty, it must either be all of X , or else it contains just one point. If $\Delta \cap X = X$, then $\Delta \supseteq X$, and so $|\Delta| \geq |X| > |\Omega|/2$. By Lemma 8.11, however, $|\Delta|$ is a divisor of $|\Omega|$, and hence in this case, $\Delta = \Omega$, which is contrary to assumption. It follows that $|\Delta \cap X| \leq 1$, as claimed.

Now suppose that Δ is an arbitrary block for the action of G on Ω . We must show that Δ is a trivial block, and so assuming that $\Delta < \Omega$, our goal is to show that $|\Delta| = 1$. By Lemma 8.11, the translates of Δ are blocks, and, of course, none of them is all of Ω . There are exactly $|\Omega|/|\Delta|$ such translates, and every point of Ω is in one of them. By the result of the previous paragraph, each translate of Δ contains at most one point of X , and thus the number of translates is at least equal to $|X|$. Then $|\Omega|/|\Delta| \geq |X| > |\Omega|/2$, and hence $|\Delta| < 2$. Thus $|\Delta| = 1$, as required. ■

Suppose that G acts transitively on Ω and let $X < \Omega$. We shall say that X is a **Jordan** set if the pointwise stabilizer G_X is transitive on $\Omega - X$, and that X is **strongly Jordan** if, in fact, G_X is primitive on $\Omega - X$. We caution the reader that this nomenclature is not standard; we have introduced it only for the material leading up to the proof of Theorem 8.18.

It should be obvious that if G acts on a set Ω and $X \subseteq \Omega$ is an orbit for some subgroup $H \subseteq G$, then for each element $g \in G$, the translate $X \cdot g$ is an orbit for the conjugate subgroup H^g . Furthermore, if H is primitive on X , then H^g is primitive on $X \cdot g$. Also, if $X \subseteq \Omega$ and $g \in G$, then

$(G_X)^g = G_{X \cdot g}$. It follows from all of this that translates of Jordan sets are Jordan, and translates of strongly Jordan sets are strongly Jordan.

8.21. Lemma. *Suppose that a group G acts transitively on Ω , and let X and Y be Jordan subsets such that $X \cup Y < \Omega$. Then $X \cap Y$ is Jordan, and if both X and Y are strongly Jordan, then $X \cap Y$ is strongly Jordan.*

Proof. First, observe that G_X and G_Y are contained in $G_{X \cap Y}$, which acts on $\Omega - (X \cap Y)$. Thus each G_X -orbit and each G_Y -orbit on the set $\Omega - (X \cap Y)$ is contained in a single $G_{X \cap Y}$ orbit. Now $\Omega - (X \cap Y) = (\Omega - X) \cup (\Omega - Y)$, and since X and Y are Jordan, it follows that $\Omega - X$ is a G_X -orbit and $\Omega - Y$ is a G_Y -orbit. To show that $G_{X \cap Y}$ is transitive on $\Omega - (X \cap Y)$, therefore, it suffices to show that $\Omega - X$ and $\Omega - Y$ are contained in the same $G_{X \cap Y}$ -orbit. This follows, however, since $(\Omega - X) \cap (\Omega - Y) = \Omega - (X \cup Y)$ is nonempty. Thus $G_{X \cap Y}$ is transitive on $\Omega - (X \cap Y)$, or in other words, $X \cap Y$ is a Jordan set, as desired.

Suppose now that both X and Y are strongly Jordan, and assume, as we may, that $|X| \leq |Y|$. Then $|\Omega - X| \geq |\Omega - Y|$, and since the sets $\Omega - X$ and $\Omega - Y$ are not disjoint, it follows that $|\Omega - X|$ is more than half the cardinality of their union, which is $\Omega - (X \cap Y)$. Now G_X stabilizes the set $\Omega - X$ and acts primitively on it, and thus by Lemma 8.20, the action of $G_{X \cap Y}$ on $\Omega - (X \cap Y)$ (which we know to be transitive) is actually primitive. It follows that $X \cap Y$ is strongly Jordan, as required. ■

Suppose that G is transitive on Ω . If $X \subseteq \Omega$ is a subset obtained by deleting one point, then obviously X is a Jordan set. Also, the empty subset of Ω is guaranteed to be Jordan. But if G is primitive on Ω and there exists a nonempty Jordan set of cardinality smaller than $|\Omega| - 1$, we get a strong conclusion: the action of G on Ω is doubly transitive.

8.22. Theorem. *Let G be a group acting primitively on Ω , and suppose that $X \subseteq \Omega$ is a Jordan set with $0 < |X| < |\Omega| - 1$. If $\alpha \in \Omega$ is arbitrary, then G_α is transitive on $\Omega - \{\alpha\}$, and so G is 2-transitive on Ω . Furthermore, if X is strongly Jordan, then in fact, G_α is primitive on $\Omega - \{\alpha\}$.*

Proof. Given the existence of the Jordan set X with $0 < |X| < |\Omega| - 1$, we show that every one-point subset of Ω is Jordan. This tells us that for each point $\alpha \in \Omega$, the stabilizer G_α is transitive on $\Omega - \{\alpha\}$, as wanted, and since G is transitive, Lemma 8.2 guarantees that G is doubly transitive in this situation. We will also show that if X is strongly Jordan, then every one-point subset of Ω is strongly Jordan, and this will complete the proof.

We can assume that X is minimal among nonempty Jordan subsets (or minimal among nonempty strongly Jordan subsets) and we work to show that $|X| = 1$. Since translates of Jordan sets are Jordan, and translates of

strongly Jordan sets are strongly Jordan, it will follow that every one-point subset of Ω is Jordan (or is strongly Jordan) as wanted.

First, assume that $|X| \geq |\Omega|/2$, and let $Y = \Omega - X$. Now $|Y| > 1$ since $|X| < |\Omega| - 1$, and we have $|Y| \leq |\Omega|/2 < |\Omega|$. Since G is primitive on Ω , it follows that Y is not a block, and hence there exists an element $g \in G$ such that $Y \cdot g \neq Y$ and $Y \cap Y \cdot g \neq \emptyset$. Now

$$X \cup X \cdot g = (\Omega - Y) \cup (\Omega - Y \cdot g) = \Omega - (Y \cap Y \cdot g),$$

and this is a proper subset of Ω . Since X is Jordan, so too is $X \cdot g$, and thus Lemma 8.21 tells us that $X \cap X \cdot g$ is Jordan. Also, if X is strongly Jordan, then by similar reasoning, $X \cap X \cdot g$ is strongly Jordan.

Now $|X| \geq |\Omega|/2 > |X \cup X \cdot g|/2$. The cardinality of each of X and $X \cdot g$, therefore, exceeds half the cardinality of their union, and it follows that $X \cap X \cdot g$ is nonempty. Furthermore, $X \neq X \cdot g$ since $Y \neq Y \cdot g$, and thus $X \cap X \cdot g < X$. Thus $X \cap X \cdot g$ is a nonempty Jordan (or strongly Jordan) set that is strictly smaller than X , and this contradicts the minimality of X .

We now have $|X| < |\Omega|/2$, and assuming that $|X| > 1$, we work to derive a contradiction. Since $1 < |X| < |\Omega|$ and G is primitive, X cannot be a block, and thus there exists $g \in G$ such that $X \neq X \cdot g$ and $X \cap X \cdot g \neq \emptyset$. Since $|X \cup X \cdot g| \leq 2|X| < |\Omega|$, we see that $X \cup X \cdot g < \Omega$, and so by Lemma 8.21, the nonempty set $X \cap X \cdot g$ is Jordan (and it is strongly Jordan if X is). This set is properly smaller than X , however, and as before, this contradicts the minimality of X . ■

Finally, we are ready to prove Jordan's theorem.

Proof of Theorem 8.18. We can assume that $|\Omega| > 2$ and that $|\Lambda| > 0$, and we proceed by induction on $|\Omega|$. By hypothesis, the set Λ is strongly Jordan, and since $|\Lambda| \leq |\Omega| - 2$, we can apply Theorem 8.22 to deduce that G_α is primitive on $\Omega - \{\alpha\}$, where we take $\alpha \in \Lambda$.

Now G_Λ is the pointwise stabilizer of the set $\Lambda - \{\alpha\}$ in G_α , and by hypothesis, G_Λ is primitive on $\Omega - \Lambda = (\Omega - \alpha) - (\Lambda - \alpha)$. Also, $|\Lambda - \{\alpha\}| \leq |\Omega - \{\alpha\}| - 2$, and so we can apply the inductive hypothesis to the action of G_α to $\Omega - \{\alpha\}$ to deduce that it is $|\Lambda|$ -transitive. By Lemma 8.2, therefore, G is $(|\Lambda| + 1)$ -transitive on Ω , as wanted. ■

Another application of Theorem 8.18 in the spirit of Theorem 8.17 and Corollary 8.19 is the following. Its proof is somewhat more difficult, however.

8.23. Theorem. *Let G be a primitive permutation group on a set Ω , and assume that G contains a p -cycle, where p is prime and $p \leq |\Omega| - 3$. Then G is either the alternating group or the full symmetric group on Ω .*

We need an easy preliminary result.

8.24. Lemma. *Let x be an n -cycle in the symmetric group S_n . Then $\langle x \rangle$ is the full centralizer of x in S_n .*

Proof. All n -cycles in S_n are conjugate, and it is easy to see that there are exactly $(n-1)!$ of them. Since the size of the conjugacy class of x in S_n is $|S_n : C|$, where C is the centralizer of x , we have $(n-1)! = n!/|C|$, and thus $|C| = n$. Since $\langle x \rangle \subseteq C$ and $|\langle x \rangle| = n$, the result follows. ■

Proof of Theorem 18.23. Let Λ be the set of points fixed by the given p -cycle, and observe that by Corollary 8.19, we can assume that $p \neq 3$. Now $|\Omega - \Lambda|$ is the prime number p , and since G_Λ contains a p -cycle, it follows that G_Λ is transitive on $\Omega - \Lambda$, and in fact it is primitive on this set. By Theorem 8.18, therefore, G is $|\Lambda|$ -transitive on Ω . (Actually, it is $(|\Lambda| + 1)$ -transitive, but we do not need that extra information.) It follows that each permutation in $\text{Sym}(\Lambda)$ is induced by some element of G , or in other words, $G_{(\Lambda)}/G_\Lambda$ is naturally isomorphic to $\text{Sym}(\Lambda)$.

Now let P be the subgroup of order p generated by the given p -cycle. Then $P \subseteq G_\Lambda$, and since G_Λ acts faithfully on the p points of $\Omega - \Lambda$, we know that $|G_\Lambda|$ divides $p!$. It follows that P is a full Sylow p -subgroup of G_Λ , and since $G_\Lambda \triangleleft G_{(\Lambda)}$, we can apply the Frattini argument to deduce that $G_{(\Lambda)} = NG_\Lambda$, where $N = \mathbf{N}_{G_{(\Lambda)}}(P)$. We conclude that $N/N_\Lambda \cong G_{(\Lambda)}/G_\Lambda \cong \text{Sym}(\Lambda)$, and thus N induces the full symmetric group on Λ .

Since $|\Lambda| = |\Omega| - p \geq 3$, it follows that $\text{Sym}(\Lambda)$ contains a 3-cycle, and it is easy to see that such a 3-cycle must lie in the derived subgroup of the symmetric group. There exists, therefore, an element $x \in N'$ such that the permutation induced by x on Λ is a 3-cycle.

The automorphism group of P is abelian, and thus N/C is abelian, where $C = \mathbf{C}_N(P)$. Then $x \in N' \subseteq C$, and so x commutes with the given p -cycle. The permutation of $\Omega - \Lambda$ induced by x , therefore, commutes with a p -cycle on these p points. By Lemma 8.23, this permutation has order dividing p , and hence x^p acts trivially on $\Omega - \Lambda$. Now x induces a 3-cycle on Λ , and since 3 does not divide p , it follows that x^p also induces a 3-cycle on Λ . At this point, we know that x^p fixes the points of $\Omega - \Lambda$ and it induces a 3-cycle on Λ . Since G acts faithfully on Ω , we see that x^p actually is a 3-cycle, and the result follows by Corollary 8.19. ■

We close this section with a result of A. Bochert that also relies on Corollary 8.19. Bochert's theorem shows that a primitive permutation group that is not either the alternating group or the full symmetric group must actually be a fairly small subgroup of the symmetric group. We begin with

an elementary (but somewhat tedious) computation that enables us to find 3-cycles in permutation groups.

8.25. Lemma. *Let x and y be permutations on a set Ω , and assume that there is exactly one point $\alpha \in \Omega$ moved by both x and y . Then the commutator $[x, y] = x^{-1}y^{-1}xy$ is a 3-cycle.*

Proof. First, we observe that α , $\alpha \cdot x$ and $\alpha \cdot y$ are three distinct points. Certainly, $\alpha \neq \alpha \cdot x$ and $\alpha \neq \alpha \cdot y$ since x and y move α . Also, since $\alpha \neq \alpha \cdot x$, we have $\alpha \cdot y \neq (\alpha \cdot x) \cdot y = \alpha \cdot x$, where the equality holds since $\alpha \cdot x$ is different from α and is moved by x , and so it is fixed by y .

Next, we show that if $\beta \in \Omega$ is not one of the three points α , $\alpha \cdot x$ or $\alpha \cdot y$, then $\beta \cdot (x^{-1}y^{-1}) = \beta \cdot (y^{-1}x^{-1})$. There is nothing to prove if both x^{-1} and y^{-1} fix β , so by symmetry, it is no loss to assume that x^{-1} moves β , and thus x moves β . Since x moves β and $\beta \neq \alpha$, we know that y fixes β , and so y^{-1} also fixes β , and we have $\beta \cdot (y^{-1}x^{-1}) = \beta \cdot x^{-1}$. Also, since x moves β , it also moves $\beta \cdot x^{-1}$, and since $\beta \cdot x^{-1} \neq \alpha$, it follows that y fixes $\beta \cdot x^{-1}$, and so y^{-1} also fixes this point. Then $\beta \cdot (x^{-1}y^{-1}) = \beta \cdot x^{-1}$, and this shows that $\beta \cdot (x^{-1}y^{-1}) = \beta \cdot (y^{-1}x^{-1})$, as claimed. It follows that

$$\beta \cdot [x, y] = \beta \cdot (x^{-1}y^{-1}xy) = \beta \cdot (y^{-1}x^{-1}xy) = \beta.$$

We have now shown that $[x, y]$ fixes every member of Ω other than α , $\alpha \cdot x$ and $\alpha \cdot y$.

Now

$$(\alpha \cdot x) \cdot [x, y] = \alpha \cdot (y^{-1}xy) = \alpha \cdot (y^{-1}y) = \alpha$$

where the second equality holds because $\alpha \cdot y^{-1}$ is moved by y and is different from α , and so it is fixed by x . It follows by interchanging the roles of x and y that $[y, x]$ carries $\alpha \cdot y$ to α , and hence $[x, y] = [y, x]^{-1}$ carries α to $\alpha \cdot y$. The points $\alpha \cdot x$, α and $\alpha \cdot y$ are distinct, and we know that $[x, y]$ carries the first of these to the second and the second to the third. Since $[x, y]$ fixes all other points in Ω , it must carry $\alpha \cdot y$ back to $\alpha \cdot x$, and so $[x, y]$ is the 3-cycle $(\alpha \cdot x, \alpha, \alpha \cdot y)$. ■

8.26. Theorem (Bochert). *Let $S = \text{Sym}(\Omega)$, where $|\Omega| = n$, and suppose G is a proper subgroup of S that is primitive on Ω . If $G \neq \text{Alt}(\Omega)$, then $|S : G| \geq [(n+1)/2]!$.*

Proof. Since the pointwise stabilizer S_Ω is trivial, there certainly exists a subset $\Delta \subseteq \Omega$ such that $S_\Delta \cap G = 1$. Choose Δ with this property so that $m = |\Delta|$ as small as possible. Now S_Δ acts faithfully on $\Omega - \Delta$, and since S is the full symmetric group on Ω , it follows that S_Δ induces the full symmetric group on $\Omega - \Delta$, and thus $|S_\Delta| = (n - m)!$.

We have

$$|S : G| \geq |S_\Delta : G \cap S_\Delta| = |S_\Delta| = (n - m)!,$$

and so it suffices to show that $m \leq n/2$, since then $n - m \geq n/2$, and thus $n - m \geq [(n + 1)/2]$.

If $m > n/2$, we will show that G contains a 3-cycle. Then since G is primitive, Corollary 8.19 asserts that G is either the alternating or symmetric group. This is contrary to assumption, however, and that will complete the proof.

Assuming that $m > n/2$, we have $|\Omega - \Delta| = n - m < m = |\Delta|$, and so by the minimality of $|\Delta|$, it follows that $G \cap S_{\Omega - \Delta}$ is nontrivial. Choose a nonidentity element $x \in G \cap S_{\Omega - \Delta}$, and let $\alpha \in \Omega$ be a point moved by x . Then α does not lie in $\Omega - \Delta$, and so $\alpha \in \Delta$.

Now $|\Delta - \{\alpha\}| < |\Delta|$, and so by another appeal to the minimality of $|\Delta|$, we can choose a nonidentity element $y \in G \cap S_{\Delta - \{\alpha\}}$. Since $G \cap S_\Delta = 1$, it follows that y does not lie in S_Δ , and thus y must move α . Thus x and y both move α , but there can be no other point moved by both x and y since if $\beta \neq \alpha$, then either $\beta \in \Omega - \Delta$, and so β is fixed by x , or else $\beta \in \Delta - \{\alpha\}$ and β is fixed by y . By Lemma 8.25, the commutator $[x, y]$ is a 3-cycle, and the proof is complete. ■

Problems 8B

8B.1. Let G be transitive on Ω , and let $\alpha \in \Omega$. Fix a nonempty subset $X \subseteq \Omega$ and let Δ be the intersection of all of those translates of X that contain α . Show that Δ is a block.

8B.2. Let G be primitive on Ω , and let $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$. If $X \subseteq \Omega$ is nonempty and proper, show that there exists an element $g \in G$ such that $\alpha \cdot g \in X$ and $\beta \cdot g \notin X$.

8B.3. Let G be a primitive permutation group on Ω , and suppose that M and N are distinct minimal normal subgroups of G . Prove that the following hold.

- (a) M and N are regular subgroups.
- (b) $M = \mathbf{C}_G(N)$ and $N = \mathbf{C}_G(M)$.
- (c) $M \cong N$.

Hint. Use Problem 8A.4.

8B.4. Let G be a solvable primitive permutation group. Show that the degree of G is a prime power and that G has a unique minimal normal subgroup.

8B.5. Let G be a primitive permutation group on Ω , and let $H = G_\alpha$ be a point stabilizer. If H has a fixed point in $\Omega - \{\alpha\}$, show that $|H| = 1$, and that G has prime order.

8B.6. Let G be a primitive permutation group on Ω , and let $H = G_\alpha$ be a point stabilizer. If H has an orbit of size 2 on $\Omega - \{\alpha\}$, show that $|H| = 2$ and that $G \cong D_{2p}$, the dihedral group of order $2p$, where $p > 2$ is a prime number.

8B.7. Let G be a primitive permutation group on Ω , and let $H = G_\alpha$ be a point stabilizer. If H has an orbit of size 3 on $\Omega - \{\alpha\}$, show that $|H|$ has the form $3 \cdot 2^e$ for some integer $e \geq 0$.

Hint. Let β lie in an H -orbit of size 3 and let $D = H_\beta$. Show that $\mathbf{O}^2(D) \triangleleft \mathbf{O}^2(K)$, where $K = \text{core}_H(D)$.

Note. By a result of C. Sims, $e \leq 4$, and so $|H|$ divides 48. Sims conjectured that if a point stabilizer in a primitive permutation group has an orbit of size r , then the order of the point stabilizer is bounded by some function of r . Sims' conjecture was eventually proved by Cameron, Praeger, Saxl and Seitz, but unfortunately their proof (which is the only one known) relies on the classification of simple groups.

8B.8. Let $x \in S_n$ be the n -cycle $(1, 2, \dots, n-1, n)$. (In other words, x carries i to $i+1$ for $1 \leq i < n$, and it carries n to 1.) Let $1 < m < n$ and suppose that $H \subseteq S_n$ is a subgroup that acts transitively on $\{1, 2, \dots, m\}$ and fixes all of the remaining points. Show that the group $G = \langle H, x \rangle$ is primitive.

Hint. Given a block Δ with $|\Delta| > 1$, show that some translate of Δ contains a point $i \leq m$ and also a point $j > m$. Deduce that that translate contains all i with $1 \leq i \leq m$.

8B.9. Let $x \in S_n$ be the n -cycle $(1, 2, \dots, n)$, and let y be the m -cycle $(1, 2, \dots, m)$, where $1 < m < n$. Show that $G = \langle x, y \rangle$ is the full symmetric group S_n if either of the integers m and n is even, and otherwise, G is the alternating group.

8B.10. Suppose that $G \subseteq S_n$ is a subgroup of index n that is not a point stabilizer. Show that $n = 6$.

Hint. Show that G is transitive, and then use Problem 8A.16 to deduce that it is 2-transitive, and thus primitive. Appeal to Bochert's theorem to deduce that $n \geq [(n+1)/2]!$. Show that the only positive integers n for which this inequality is valid are 1, 2, 3, 4 and 6.

Note. The symmetric group S_6 actually does have a subgroup of index 6 that does not stabilize a point. To see this, observe that S_5 acts transitively on its six Sylow 5-subgroups. It is not hard to show that this is a faithful action, and thus S_5 can be embedded as a transitive subgroup of S_6 , and of course, this copy of S_5 in S_6 has index 6 and does not stabilize a point.

Note also that if S_n has a non-inner automorphism σ , then σ would carry a point stabilizer to a subgroup of index n that is not a point stabilizer, and by this problem, that cannot happen unless $n = 6$. It follows that all automorphisms of S_n are inner for $n \neq 6$. Furthermore, it is easy to show that a subgroup H of index 6 in S_6 that does not stabilize a point has trivial core, and thus there is an injective homomorphism from S_6 to S_6 that maps H to a point stabilizer. This map is a non-inner automorphism of S_6 .

8C

Throughout much of this book we have sought results that could be used to prove that a group is not simple, but in this section, we will use some permutation-group theory to prove that certain groups actually are simple. We begin with a comparatively easy result of this type.

8.27. Theorem. *If $n \geq 5$, the alternating group A_n is simple.*

Proof. Assuming that $1 < N \triangleleft A_n$, we work to show that $N = A_n$. Since A_n is $(n-2)$ -transitive in its natural action, it is certainly 2-transitive, and thus it is primitive by Lemma 8.16. By Lemma 8.15, therefore, N acts transitively.

Suppose first that $n = 5$. Since N acts transitively on a set of cardinality 5, we deduce that 5 divides $|N|$. But $|A_5| = 60$, and so $|A_5 : N|$ is not divisible by 5, and thus all 5-cycles in A_5 lie in N . The number of these 5-cycles is 24, and thus $|N| \geq 24$. Since $|N|$ divides 60, the only possibilities are $|N| = 30$ or $|N| = 60$, and, in particular, $|A_5 : N|$ is not divisible by 3. Then all 3-cycles in A_5 lie in N , and we count that there are 20 of these. Since N contains all 5-cycles and all 3-cycles, we have $|N| \geq 24 + 20 = 44$. The only possibility is that $|N| = 60$, and thus $N = A_5$ and A_5 is simple.

We can now suppose that $n \geq 6$, and we proceed by induction on n to derive a contradiction if $N < A_n$. Let H be a point stabilizer in A_n , and observe that $H \cong A_{n-1}$, and so H is simple by the inductive hypothesis. Also, since N is transitive, we have $NH = A_n$ by Lemma 8.5. Then $H \not\subseteq N$ since otherwise, we would have $N = A_n$, which we are assuming is not the case. It follows that $N \cap H$ is a proper normal subgroup of H , and since H is simple, we have $N \cap H = 1$. Since N is transitive, it follows that it is a regular normal subgroup of A_n , and by Lemma 8.5, the conjugation

action of H on the nonidentity elements of N is permutation-isomorphic to the natural action of $H \cong A_{n-1}$ on $n-1$ points. Then $|N| = n$, and the action of H on its nonidentity elements is $(n-3)$ -transitive, and, in particular, it is 3-transitive. However, this is impossible since by Lemma 8.8(c), the 3-transitive action of H on the nonidentity elements of N would force $|N| = 4$. ■

8.28. Corollary. *If $n \geq 5$, the symmetric group S_n has exactly three normal subgroups: the identity, the whole group and A_n .*

Proof. Suppose $N \triangleleft S_n$ and that N is not one of A_n or S_n . Then $N \not\supseteq A_n$, and thus $N \cap A_n$ is a proper normal subgroup of the simple group A_n . It follows that $N \cap A_n = 1$, and thus $|N| \leq |S_n : A_n| = 2$. Since S_n is n -transitive on n -points, it is primitive, and thus if $N > 1$, then N is transitive and $|N| \geq n$. This is not the case, however, and so $N = 1$. ■

We turn now to the projective special linear groups $PSL(n, q)$. Recall that by definition, $PSL(n, q) = SL(n, q)/Z$, where Z is the central subgroup of $SL(n, q)$ consisting of the scalar matrices with determinant equal to 1. We begin work now toward a proof that with just two exceptions, all of the groups $PSL(n, q)$ are simple for prime powers q and integers $n \geq 2$. The exceptions are $PSL(2, 2)$ and $PSL(2, 3)$, which are not simple. (In fact, these two groups are solvable since $PSL(2, 2)$ has order 6 and is isomorphic to the symmetric group S_3 , and $PSL(2, 3)$ has order 12 and is isomorphic to the alternating group A_4 .) Actually, the groups $PSL(n, F)$ are also simple when F is an infinite field. Although the proof that we will present for finite fields goes through without essential modification for infinite fields too, we will nevertheless limit our discussion to the finite case.

Assuming that $n \geq 2$ (as we will, throughout this discussion), it follows by Lemma 8.3 that $SL(n, q)$ acts 2-transitively on the set Ω of one-dimensional subspaces of a vector space V of dimension n over the field F of order q . Since the action of a scalar matrix on the vector space V is just scalar multiplication, the subgroup Z acts trivially on Ω . Thus Z is contained in the kernel of the action, and we can view $PSL(n, q) = SL(n, q)/Z$ as acting on Ω . In fact, this action is faithful.

8.29. Lemma. *For all integers $n \geq 2$ and all prime powers q , the group $PSL(n, q)$ is a 2-transitive permutation group of degree $(q^n - 1)/(q - 1)$.*

Proof. We know that $PSL(2, q)$ acts on the set Ω of one-dimensional subspaces of the n -dimensional space V over the field F of order q . Now V contains exactly $q^n - 1$ nonzero vectors, and each of these lies in a unique one-dimensional subspace. Since each such subspace contains exactly $q - 1$ nonzero vectors, it follows that $|\Omega| = (q^n - 1)/(q - 1)$.

It remains to show that $PSL(n, q)$ acts faithfully on Ω , or equivalently, that Z is the full kernel of the action of $SL(n, q)$ on Ω . To see this, let $x \in SL(n, q)$ lie in the kernel of the action. Then x fixes every one-dimensional subspace of V , and thus x carries every vector $v \in V$ to some scalar multiple of itself.

Let $\{v_i \mid 1 \leq i \leq n\}$ be a basis for V , and write $(v_i)x = \alpha_i v_i$ for appropriate scalars $\alpha_i \in F$. Then x corresponds to a diagonal matrix, and to complete the proof, it suffices to show that $\alpha_i = \alpha_j$ for $1 \leq i < j \leq n$. Now for some scalar $\alpha \in F$, we have

$$\alpha(v_i + v_j) = (v_i + v_j)x = v_i x + v_j x = \alpha_i v_i + \alpha_j v_j,$$

and since v_i and v_j are linearly independent, this yields $\alpha_i = \alpha = \alpha_j$, as required. ■

Recall that a group G is said to be perfect if $G' = G$. Also, if $S \subseteq G$ is an arbitrary subgroup, then the normal closure of S in G is the subgroup $S^G = \langle S^g \mid g \in G \rangle$; it is the unique smallest normal subgroup of G that contains S . Of course, if G is a nonabelian simple group, then G is perfect and $S^G = G$ for every nontrivial subgroup S . Conversely, if G is perfect and it is the normal closure of an appropriate subgroup, and if, in addition, G is a primitive permutation group, our next result guarantees that G is simple. Since $PSL(n, q)$ is a doubly transitive permutation group by Lemma 8.29, it is certainly a primitive permutation group, and hence the following lemma of K. Iwasawa is relevant to establishing the simplicity of this group.

8.30. Lemma (Iwasawa). *Let G be a primitive permutation group, and assume that $G' = G$. Let $H = G_\alpha$ be a point stabilizer in G , and suppose that there exists a solvable subgroup $A \triangleleft H$ such that $G = A^G$. Then G is simple.*

Proof. Let $1 < N \triangleleft G$, and observe that since G is a primitive permutation group, N is transitive, and thus $NH = G$. Now $N \triangleleft G$, and since $A \triangleleft H$, we see that $H \subseteq \mathbf{N}_G(NA)$. Also $N \subseteq \mathbf{N}_G(NA)$, and thus since $NH = G$, we have $NA \triangleleft G$. Now $A^G = G$ and $A \subseteq NA \triangleleft G$, and it follows that $NA = G$. But A is solvable, so G/N must also be solvable, and hence if $N < G$, we have $(G/N)' < G/N$. Since $G' = G$, however, we see that $(G/N)' = G/N$, and this contradiction shows that $N = G$. This completes the proof. ■

We will use Lemma 8.30 to prove that a group of the form $G = PSL(n, q)$ is simple (except when $n = 2$ and $q \leq 3$). To do this, we will establish (in the non-exceptional cases) that $G' = G$, and we will find a solvable (and, in fact, an abelian) normal subgroup A of a point stabilizer, such that $A^G = G$. (Note that the groups $PSL(2, 2)$ and $PSL(2, 3)$ definitely are not perfect

since they are solvable.) The key to both of these tasks is to consider certain special matrices $t_{i,j}(\alpha)$ in $SL(n, q)$.

To define the matrices $t_{i,j}(\alpha)$ and to facilitate matrix computations, we recall that the **matrix unit** $e_{i,j}$ is the matrix whose only nonzero entry is 1, occurring in the (i, j) -position. It is trivial to check that matrix units multiply according to the formula

$$e_{i,j}e_{u,v} = \begin{cases} e_{i,v} & \text{if } j = u \\ 0 & \text{otherwise.} \end{cases}$$

It is the simplicity of this rule that makes the matrix units so useful for computation.

Given $1 \leq i, j \leq n$ with $i \neq j$, define $t_{i,j}(\alpha) = 1 + \alpha e_{i,j}$, where, in this formula, 1 is the $n \times n$ identity matrix and $\alpha \in F$ is nonzero. Clearly, $t_{i,j}(\alpha)$ is either upper or lower triangular (depending on whether $i < j$ or $i > j$) and its diagonal entries are all 1. The determinant of this matrix, therefore, is 1, and so $t_{i,j}(\alpha) \in SL(n, q)$, as wanted.

We digress briefly to put our matrices $t_{i,j}(\alpha)$ into a somewhat more general context. Let V be a vector space of dimension $n \geq 2$. A **hyperplane** in V is a subspace of dimension $n - 1$, or equivalently, a subspace of codimension 1. A linear operator t on V is a **transvection** if its fixed-point space is a hyperplane W , and t acts as the identity on V/W . It is not hard to show that all of our matrices $t_{i,j}(\alpha)$ are transvections and also that the transvections in $GL(n, q)$ form a single conjugacy class. In particular, all of the transvections in $GL(n, q)$ actually lie in $SL(n, q)$, and one can show that if $n \geq 3$, all of these transvections are conjugate in $SL(n, q)$.

We return now to work toward our main goal, which is the proof that the groups $PSL(n, q)$ are simple (except when they are not).

8.31. Theorem. *Let $n \geq 2$. Then the group $SL(n, q)$ is generated by the matrices $t_{i,j}(\alpha)$ with $i \neq j$ and $\alpha \neq 0$.*

Proof. If a is any $n \times n$ matrix over the field F of order q , it is easy to see that the product matrix $t_{i,j}(\alpha)a$ can be obtained from a by adding α times row j to row i , and, similarly, the matrix $at_{i,j}(\alpha)$ can be obtained from a by adding α times column i to column j . We describe an algorithm by which an arbitrary matrix $a \in SL(n, q)$ can be converted into the identity matrix by a sequence of row and column operations of these types, and it follows that $1 = paq$, where each of p and q is a product of matrices of the form $t_{i,j}(\alpha)$. This will prove the result.

Let $a \in SL(n, q)$. The first column of a is not zero, and since $n \geq 2$, some row operation of the above type (if necessary) will convert a to a matrix in which the $(i, 1)$ -entry is a nonzero field element δ , where $i > 1$. Assuming

that has been done, let γ be the $(1, 1)$ -entry of the resulting matrix, where possibly, $\gamma = 0$. If we add $(1 - \gamma)/\delta$ times row i to row 1, we obtain a matrix with $(1, 1)$ -entry equal to 1. Now a sequence of additions of appropriate multiples of the first row to other rows will yield a matrix with $(1, 1)$ -entry equal to 1 and all other entries in the first column equal to 0, and then a sequence of additions of appropriate multiples of the first column to other columns will yield a matrix where the $(1, 1)$ -entry is 1 and all other entries in the first row and first column are 0.

Observe that the matrix constructed in the previous paragraph has determinant 1 since a and all of the matrices $t_{i,j}(\alpha)$ have determinant 1. We change notation now, and call this new matrix a . If $n = 2$, then a is diagonal, and since its $(1, 1)$ entry is 1 and its determinant is 1, the $(2, 2)$ -entry of a must also be 1, and thus a is the identity matrix, as wanted. Assume then, that $n \geq 3$. Since some entry in column 2 is nonzero, we can do row and column operations as before, but using only rows and columns numbered 2 or larger. This will not change either the first row or the first column of a , but we can arrange that the $(2, 2)$ -entry of the resulting matrix is 1, and that all other entries in the second row and second column are 0.

If $n = 3$, the resulting matrix is diagonal, and so it is the identity matrix by the determinant argument that we used before. If $n > 3$, we again do row and column operations, but this time with rows and columns numbered 3 or higher. Continuing like this, we eventually obtain the identity matrix, and this completes the proof. ■

8.32. Theorem. *If $n \geq 3$ or $n = 2$ and $q > 3$, then $SL(n, q)$ is perfect.*

Proof. By Theorem 8.31, it suffices to show that the matrix $t_{i,j}(\alpha)$ is a commutator, where $i \neq j$ and $\alpha \neq 0$. We begin with the observation that if $i \neq j$, then $(e_{i,j})^2 = 0$. Then $(1 - \alpha e_{i,j})(1 + \alpha e_{i,j}) = 1$, and hence $(1 + \alpha e_{i,j})^{-1} = 1 - \alpha e_{i,j}$.

Suppose first that $n \geq 3$, and let $1 \leq i, j, k \leq n$, where i, j and k are distinct. Then

$$(e_{i,k})^{1+\alpha e_{k,j}} = (1 - \alpha e_{k,j})(e_{i,k})(1 + \alpha e_{k,j}) = e_{i,k} + \alpha e_{i,j},$$

and thus

$$(1 + e_{i,k})^{1+\alpha e_{k,j}} = 1 + e_{i,k} + \alpha e_{i,j}.$$

It follows that

$$\begin{aligned} [(1 + e_{i,k}), (1 + \alpha e_{k,j})] &= (1 + e_{i,k})^{-1}(1 + e_{i,k})^{1+\alpha e_{k,j}} \\ &= (1 - e_{i,k})(1 + e_{i,k} + \alpha e_{i,j}) \\ &= 1 + \alpha e_{i,j} \\ &= t_{i,j}(\alpha), \end{aligned}$$

and thus $t_{i,j}(\alpha)$ is a commutator, as wanted.

We can now assume that $n = 2$, and we let $\beta, \gamma \in F$ be nonzero. Let

$$b = \begin{bmatrix} \beta^{-1} & 0 \\ 0 & \beta \end{bmatrix} \quad \text{and} \quad c = \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix},$$

so that b and c lie in $SL(2, q)$. Then

$$\begin{aligned} [b, c] &= \begin{bmatrix} \beta^{-1} & 0 \\ 0 & \beta \end{bmatrix}^{-1} \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} \beta^{-1} & 0 \\ 0 & \beta \end{bmatrix} \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix} \\ &= \left(\begin{bmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{bmatrix} \begin{bmatrix} 1 & -\gamma \\ 0 & 1 \end{bmatrix} \right) \left(\begin{bmatrix} \beta^{-1} & 0 \\ 0 & \beta \end{bmatrix} \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix} \right) \\ &= \begin{bmatrix} \beta & -\beta\gamma \\ 0 & \beta^{-1} \end{bmatrix} \begin{bmatrix} \beta^{-1} & \beta^{-1}\gamma \\ 0 & \beta \end{bmatrix} \\ &= \begin{bmatrix} 1 & \gamma(1 - \beta^2) \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Now let α be an arbitrary nonzero element of F . If $q > 3$, choose $\beta \neq \pm 1$. Then $1 - \beta^2 \neq 0$, and so we can choose γ so that $\gamma(1 - \beta^2) = \alpha$. Then $[b, c] = t_{1,2}(\alpha)$, and so $t_{1,2}(\alpha)$ is a commutator in $SL(2, q)$, as wanted. By taking transposes, we see that $t_{2,1}(\alpha)$ is also a commutator in $SL(2, q)$, and this completes the proof. ■

We can now establish the main result of this section.

8.33. Theorem. *If $n \geq 3$ or $n = 2$ and $q > 3$, then $PSL(n, q)$ is simple.*

Proof. Using the bar convention, we can write $PSL(n, q) = \bar{S} = S/Z$, where $S = SL(n, q)$ and Z is the group of scalar matrices in S . Let V be the n -dimensional row space over F , and let $\{v_i \mid 1 \leq i \leq n\}$ be the standard basis for V , so that v_i is the row vector $(0, \dots, 0, 1, 0, \dots, 0)$, whose only nonzero entry is in position i . Now S acts by right multiplication on V , and the corresponding action of \bar{S} on the set Ω of one-dimensional subspaces of V is faithful and doubly transitive by Lemma 8.29. In particular, \bar{S} is a primitive permutation group on Ω . Also, since S is perfect by Theorem 8.32, we have $(\bar{S})' = \bar{S}' = \bar{S}$, and so \bar{S} is perfect.

Now fix an integer j with $1 \leq j \leq n$, and let H_j be the stabilizer in $SL(n, q)$ of the one-dimensional space $U_j = Fv_j$. Then H_j acts on the vector space V/U_j , and this induces a group homomorphism from H_j into the group $GL(V/U_j)$ of invertible linear operators on V/U_j . Let A_j be the kernel of this homomorphism, so that A_j is the group of all matrices in $SL(n, q)$ that stabilize U_j and act trivially on V/U_j . In particular, if $a \in A_j$, then $\det(a) = 1$, and since the linear transformation induced by a on V/U_j is the identity map, it too has determinant 1. It follows that the

linear transformation of U_j induced by a also has determinant 1. The map induced by a on the one-dimensional space U_j is thus the identity map, and so $(v_j)a = v_j$. Also, since a fixes every element of V/U_j , we see that if $i \neq j$ then $(v_i)a = v_i + \beta_i v_j$ for some scalar β_i depending on i . In other words,

$$a = 1 + \sum_{i \neq j} \beta_i e_{i,j},$$

and it is easy to see that A_j is exactly the set of matrices of this form. It follows by the multiplication rule for matrix units that A_j is an abelian group, and, of course, $A_j \triangleleft H_j$ since A_j is the kernel of a homomorphism defined on H_j . Notice also that the matrices $t_{i,j}(\alpha)$ lie in A_j , for $i \neq j$.

Now $S = SL(n, q)$ acts transitively on the set of one-dimensional subspaces of V , and since the group A_j is uniquely determined by the space $U_j = Fv_j$, it follows that all of the abelian groups A_j are conjugate in S . (We are not saying, however, that they form a full conjugacy class of subgroups.) Every matrix of the form $t_{i,j}(\alpha)$ lies in one of the conjugate subgroups A_j , and since these matrices generate S by Theorem 8.31, it follows that $(A_1)^S = S$.

Now $\overline{H_1}$ is a point stabilizer in the primitive group \overline{S} , and $\overline{A_1}$ is a solvable (and in fact abelian) normal subgroup of $\overline{H_1}$. (It is irrelevant that A_1 usually does not contain Z .) Also, $(\overline{A_1})^{\overline{S}} = \overline{(A_1)^S} = \overline{S}$. Since \overline{S} is perfect, it follows by Lemma 8.30 that it is simple. ■

We mention that the simplicity of $PSL(n, q)$ implies that the scalar subgroup $Z \subseteq SL(n, q)$ is actually the full center of $SL(n, q)$.

Problems 8C

8C.1. Show that A_6 has no subgroup of order 120, and deduce that a group of order 120 cannot be simple.

Note. There does exist a perfect group of order 120, however: $SL(2, 5)$.

8C.2. Suppose that G is a permutation group of degree 11 and order $7920 = 11 \cdot 10 \cdot 9 \cdot 8$. Prove that G is simple.

Hint. Show that $|\mathbf{N}_G(P)| = 55$, where $P \in \text{Syl}_1(G)$.

Note. In fact, G must be isomorphic to the Mathieu group M_{11} .

8C.3. Suppose that G is a transitive permutation group of degree 12 and order $95,040 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$. Prove that G is simple.

Hint. Show that G must be 2-transitive, and that a nonidentity proper normal subgroup would have to be regular. Observe that a group of order 12 can never be a minimal normal subgroup of any group.

Note. In fact, G must be isomorphic to the Mathieu group M_{12} .

8C.4. Let G be a transitive group of degree 100 on a set Ω , and suppose that a point stabilizer G_α is simple, and that it has orbits of size 22 and 77 on $\Omega - \{\alpha\}$. Show that G is primitive, and deduce that it is simple.

Note. The Higman-Sims group HS satisfies these conditions, and, in that case, the point stabilizer H is isomorphic to the Mathieu group M_{22} .

8C.5. Let G be a 5-transitive group of degree 24, and assume that the setwise stabilizer of three points is simple. Prove that the stabilizer in G of two points, the stabilizer in G of one point and G itself are simple groups.

Note. This problem describes the Mathieu groups M_{22} , M_{23} and M_{24} . The three-point stabilizer is isomorphic to $PSL(3, 4)$, acting 2-transitively on $21 = (4^3 - 1)/(4 - 1)$ points, as in Lemma 8.29.

8C.6. Let A be an abelian group. Show that $\text{Aut}(A)$ is simple if and only if A has order 3 or A is an elementary abelian 2-group of order at least 8.

8D

We assume throughout this section that G acts transitively on Ω , and we study the orbits of the action of a point stabilizer on Ω . As we shall see, a good way to understand these **suborbits** is to consider the natural componentwise action of G on the set $\Omega \times \Omega$ of ordered pairs of points, where this action is defined by the formula $(\alpha, \beta) \cdot g = (\alpha \cdot g, \beta \cdot g)$.

The set $\Omega \times \Omega$ is partitioned into G -orbits, which are usually called **orbitals**. One of these is the **diagonal** $\{(\alpha, \alpha) \mid \alpha \in \Omega\}$. (The diagonal is certainly G -invariant, and it is a single G -orbit because G is transitive on Ω .) If $|\Omega| > 1$, the diagonal obviously does not exhaust $\Omega \times \Omega$, and so the total number of G -orbits on this set (in other words, the total number of orbitals) is at least 2. The number of orbitals is the **rank** of the action, which is defined only for transitive actions. If Δ is an orbital, it is obvious that the set

$$\Delta' = \{(\beta, \alpha) \mid (\alpha, \beta) \in \Delta\}$$

is also an orbital, and we say that Δ and Δ' are **paired** orbitals. Of course, an orbital may be paired with itself. For example, the diagonal orbital is self-paired, and if the rank is 2, there is only one other orbital, so it too must be self-paired.

A transitive action of G on Ω has rank 2 precisely when $|\Omega| > 1$ and G acts transitively on the set of all of pairs in $\Omega \times \Omega$ that lie outside of the diagonal. These, of course, are exactly the pairs of *distinct* points in Ω , and we recall that by definition, G is doubly transitive on Ω if and only if it

acts transitively on this set of pairs. In other words, a transitive action is 2-transitive if and only if it has rank 2.

If G has rank 2 on Ω , it is 2-transitive, and, in this case, we know that a point stabilizer G_α has exactly two orbits on Ω , namely, $\{\alpha\}$ and $\Omega - \{\alpha\}$. More generally, we shall see that the number of G_α -orbits on Ω is always equal to the rank.

It should not be surprising that the number of orbits of G_α on Ω is independent of the choice of α since by transitivity, the various point stabilizers are conjugate in G . We might even expect that the sizes of these suborbits correspond as α varies. In fact, even more is true. Given points $\alpha, \beta \in \Omega$, there is a natural, size-preserving bijection between the sets of G_α -orbits and G_β -orbits on Ω . To define this bijection, we introduce some notation.

Let Δ be an orbital. We write

$$\Delta(\alpha) = \{\beta \in \Omega \mid (\alpha, \beta) \in \Delta\},$$

so that the orbital Δ defines a function from Ω into the set of all subsets of Ω . These **orbital functions** are intimately connected with the suborbits.

8.34. Lemma. *Let G be a group acting transitively on Ω , and let α in Ω . Then as Δ runs over the orbitals, the sets $\Delta(\alpha)$ are disjoint, and they are exactly the orbits of G_α on Ω . Also, if $g \in G$, then for each orbital Δ , we have $\Delta(\alpha \cdot g) = \Delta(\alpha) \cdot g$. In particular $|\Delta(\alpha)|$ is independent of $\alpha \in \Omega$, and, in fact, $|\Delta(\alpha)| = |\Delta|/|\Omega|$.*

Proof. Suppose that $\Delta_1(\alpha)$ and $\Delta_2(\alpha)$ have some point β in common, where Δ_1 and Δ_2 are orbitals. This means that the pair (α, β) lies in each of the sets Δ_1 and Δ_2 , and since these sets are G -orbits on $\Omega \times \Omega$ and they are not disjoint, they must be equal. It follows that the sets $\Delta(\alpha)$ are disjoint for distinct orbitals Δ .

Now let $g \in G$, and suppose Δ is an orbital. Since Δ is a G -invariant subset of $\Omega \times \Omega$, it follows that $(\alpha, \beta) \in \Delta$ if and only if $(\alpha \cdot g, \beta \cdot g) \in \Delta$. Equivalently, $\beta \in \Delta(\alpha)$ if and only if $\beta \cdot g \in \Delta(\alpha \cdot g)$, and this proves that $\Delta(\alpha \cdot g) = \Delta(\alpha) \cdot g$, as wanted. Also, since $\alpha \cdot g$ runs over all of Ω as g varies, it follows that for a fixed orbital Δ , all of the sets $\Delta(\alpha)$ have equal cardinality.

If $g \in G_\alpha$, we have $\Delta(\alpha) \cdot g = \Delta(\alpha \cdot g) = \Delta(\alpha)$, and thus $\Delta(\alpha)$ is a G_α -invariant subset of Ω . To show that it is actually a G_α -orbit, let $\beta, \gamma \in \Delta(\alpha)$. Then (α, β) and (α, γ) lie in Δ , which is a G -orbit on $\Omega \times \Omega$. There exists, therefore, an element $g \in G$ that carries (α, β) to (α, γ) . Then $\beta \cdot g = \gamma$, and since $\alpha \cdot g = \alpha$, we have $g \in G_\alpha$, as wanted.

Finally, for $\alpha \in \Omega$, we see that $|\Delta(\alpha)|$ is exactly the number of pairs in Δ whose first entry is α , and thus

$$|\Delta| = \sum_{\alpha \in \Omega} |\Delta(\alpha)|.$$

But $|\Delta(\alpha)|$ is independent of α , and this yields $|\Delta| = |\Omega||\Delta(\alpha)|$. ■

As we indicated, Lemma 8.34 establishes a natural bijection from the set of G_α -orbits on Ω onto the set of G_β -orbits on Ω , where $\alpha, \beta \in \Omega$. Given a G_α -orbit X , we know that $X = \Delta(\alpha)$ for some unique orbital Δ , and we let X correspond to the G_β -orbit $Y = \Delta(\beta)$. In fact, given X , it is easy to determine Y without knowing the orbital Δ . This is because $\beta = \alpha \cdot g$ for some element $g \in G$, and so

$$Y = \Delta(\beta) = \Delta(\alpha \cdot g) = \Delta(\alpha) \cdot g = X \cdot g.$$

The cardinalities of the orbits of G_α for any given point α are called the **subdegrees** of G , and this list of positive integers is independent of the choice of α . Also, at least one of the subdegrees is the number 1 since $\{\alpha\}$ is an orbit of G_α . (Note that this trivial G_α -orbit is $\Delta(\alpha)$, where Δ is the diagonal orbital.)

In fact, the corresponding orbits X and Y for G_α and G_β share more than cardinalities. Fix $g \in G$ carrying α to β . Then the isomorphism $u \mapsto u^g$ from G_α to G_β and the bijection $x \mapsto x \cdot g$ from X to Y are compatible in the sense that

$$(x \cdot u) \cdot g = (x \cdot g) \cdot u^g.$$

It is easy to see from this that a property such as primitivity, 2-transitivity, faithfulness, *etc.* holds for the action of G_α on X if and only if it holds for the action of G_β on Y . (We hope that the reader will forgive us for omitting a formal proof of this.)

A useful way to think about orbitals is via graph theory. We can view an orbital Δ as the set of edges of a directed graph with vertex set Ω . To do this, we imagine Ω to be set of points in space, and we draw an arrow from α to β precisely when the pair (α, β) lies in Δ . (This is not very interesting if Δ is the diagonal, but in all other cases, each arrow joins a pair of distinct points.) The graph constructed in this way is the **orbital graph** associated with Δ , and we will refer to its edges Δ -arrows.

Since every ordered pair of points in Ω lies in exactly one orbital, it follows that for each such pair (α, β) , there is a unique orbital Δ such that Δ -arrow goes from α to β . Perhaps a good way to think about this is to imagine the orbitals as colors. There is an arrow joining α to β for every choice of $\alpha, \beta \in \Omega$, and the “color” of that arrow is determined by the orbital

that contains the corresponding pair (α, β) . (This point of view is convenient when we need to think about two or more orbital graphs simultaneously.)

Observe that for each orbital Δ , the set of points reached by Δ -arrows leaving α is exactly $\Delta(\alpha)$. Also, and most importantly, if there is a Δ -arrow from α to β , then there is also a Δ -arrow from $\alpha \cdot g$ to $\beta \cdot g$. (This, of course, is because Δ is a G -invariant subset of $\Omega \times \Omega$.) It follows that the given action of G on Ω defines automorphisms of each of the orbital graphs. Of course, G acts transitively on the points in the Δ -graph, but it also is edge-transitive because Δ is a G -orbit on $\Omega \times \Omega$.

The following result provides a pretty connection between the graph theory and the group theory.

8.35. Theorem. *Let G be a group acting transitively on Ω . Then G is primitive if and only if the graph associated with every non-diagonal orbital is connected.*

The statement of Theorem 8.35 is ambiguous since there are two different notions of connectivity relevant to directed graphs. A directed graph is **path connected** if given any two vertices α and β , there is a sequence of vertices $\alpha = \alpha_0, \alpha_1, \dots, \alpha_k = \beta$ such that for $0 \leq i < k$, there is an arrow $\alpha_i \rightarrow \alpha_{i+1}$. The graph is **topologically connected** if such a sequence of vertices exists and for $0 \leq i < k$, there is either an arrow $\alpha_i \rightarrow \alpha_{i+1}$ or there is an arrow $\alpha_{i+1} \rightarrow \alpha_i$. (Of course, a path-connected graph is topologically connected, but in general, the converse is false.) Fortunately, in the presence of sufficient symmetry, the two concepts coincide.

8.36. Lemma. *Let \mathcal{G} be a finite directed graph, and suppose that \mathcal{G} is topologically connected. If the automorphism group of \mathcal{G} is transitive on vertices, then \mathcal{G} is path connected.*

Proof. It suffices to show that if $\beta \rightarrow \alpha$ in \mathcal{G} , then there is a path (following arrows) from α to β . Let g be an automorphism of \mathcal{G} such that $\beta \cdot g = \alpha$, and suppose that g has order n . Since g is a graph automorphism, we have $\alpha = \beta \cdot g \rightarrow \alpha \cdot g$, and thus $\alpha \cdot g^i \rightarrow \alpha \cdot g^{i+1}$ for all integers i . This yields the path

$$\alpha \rightarrow \alpha \cdot g \rightarrow \alpha \cdot g^2 \rightarrow \dots \rightarrow \alpha \cdot g^{n-1} = \alpha \cdot g^{-1} = \beta,$$

and this completes the proof. ■

In the situation of Theorem 8.35, the group G acts on each orbital graph via graph automorphisms, and it is transitive on the vertex set Ω . By Lemma 8.36, therefore, there is no real ambiguity in the statement of 8.35.

Proof of Theorem 8.35. First, assume that each nondiagonal orbital graph is connected, and suppose $X \subseteq \Omega$ is a nontrivial block. Choose distinct

points α and $\beta \in X$, and let Δ be the orbital that contains the pair (α, β) , so that Δ is not the diagonal. By assumption, the orbital graph corresponding to Δ is path connected, and since $X < \Omega$, there must be a Δ -arrow leaving X . Let $\gamma \rightarrow \delta$ be a Δ -arrow with $\gamma \in X$ and $\delta \notin X$. Then both (α, β) and (γ, δ) lie in Δ , and hence there exists $g \in G$ carrying (α, β) to (γ, δ) . Now $\gamma \in X$ and also $\gamma = \alpha \cdot g \in X \cdot g$, so X and $X \cdot g$ are not disjoint. But X is a block, and thus

$$\delta = \beta \cdot g \in X \cdot g = X.$$

This is a contradiction, and hence G is primitive.

Conversely, suppose that G is primitive, and fix a non-diagonal orbital Δ . The orbital graph of Δ can be decomposed into disjoint topologically connected components. These components are permuted by the graph automorphisms induced by elements of G , and it follows that each component is a block. But Δ is not the diagonal, and hence each point is joined by a Δ -arrow to some other point. A connected component X of the corresponding orbital graph thus contains more than one point, and by primitivity, it follows that $X = \Omega$. The graph is thus topologically connected, and hence it is path connected too. ■

Finally, we are ready to use this graph-theoretic point of view to establish some results about suborbits and subdegrees of primitive actions.

8.37. Theorem. *Let G be a group acting primitively on Ω , and suppose that the subdegrees are $1 = m_1 \leq m_2 \leq \dots \leq m_r$, where r is the rank. Then for $1 \leq i < r$, we have $m_{i+1}/m_i \leq m_2$.*

Proof. Let $\alpha \in \Omega$, and let Δ be an orbital with $|\Delta(\alpha)| = m_2$. Since we can assume that Δ is not the diagonal, the corresponding orbital graph is path connected, and so for each point $\beta \in \Omega$, there is a path (following Δ -arrows) from α to β . Write $d(\beta)$ to denote the length of the shortest such path, so that for example, $d(\alpha) = 0$, and $d(\beta) = 1$ precisely when $\beta \in \Delta(\alpha)$.

Now let $i < r$. If $m_i = m_{i+1}$, there is nothing to prove, so we can assume that $m_{i+1} > m_i$, and hence there is at least one G_α -orbit of size exceeding m_i . Let β lie in one of these large G_α -orbits, and choose β so that $d = d(\beta)$ is as small as possible. Observe that $d > 1$ because otherwise, β is either equal to α or else it lies in $\Delta(\alpha)$, and in either case it lies in a G_α -orbit of size at most m_2 , which does not exceed m_i . It follows that there exists a point γ , where $d(\gamma) = d - 1$ and there is a Δ -arrow $\gamma \rightarrow \beta$.

Now let X and Y be the unique orbitals such that $(\alpha, \gamma) \in X$ and $(\alpha, \beta) \in Y$. By the choice of β , we have $|Y(\alpha)| > m_i$, and so $|Y(\alpha)| \geq m_{i+1}$. Also, we have $|X(\alpha)| \leq m_i$ by the minimality of d .

One can travel from α to β by first traversing the X -arrow from α to γ , and then the Δ -arrow from γ to β . Since G_α fixes α and induces automorphisms of both the X -graph and the Δ -graph, it follows that one can travel from α to an arbitrary point in the G_α -orbit of β by first traversing some X -arrow and then some Δ -arrow. In other words, every point in $Y(\alpha)$ can be reached in this way.

The number of X -arrows leaving α is $|X(\alpha)| \leq m_i$, and the number of Δ -arrows leaving each point in Ω is m_2 . It follows that the number of different points that can be reached from α by first traversing an X -arrow and then a Δ -arrow is at most $m_2 m_i$. We now have

$$m_{i+1} \leq |Y(\alpha)| \leq m_2 m_i,$$

and the result follows. ■

Note that if $m_2 = 1$ in Theorem 8.37, then all G_α -orbits have size 1, which means that G_α acts trivially on Ω . Thus if G is a primitive permutation group and a point stabilizer fixes a second point, then the point stabilizer is the trivial subgroup. By primitivity, however, the point stabilizer is a maximal subgroup, and thus $|G|$ is prime. But of course, one does not really need anything as sophisticated as Theorem 8.37 to obtain this conclusion, which is Problem 8B.5.

Next, we give another necessary condition for a list of positive integers to be the subdegrees of a primitive action.

8.38. Theorem (Weiss). *Let G be a group acting primitively on Ω , and let n be the largest subdegree. If m is a subdegree coprime to n , then $m = 1$.*

It is convenient to introduce a little more notation. Suppose that $\alpha, \beta \in \Omega$, where, as usual, G is transitive on Ω . Then the pair (α, β) lies in some orbital Δ , and in this situation, we have said that $\alpha \rightarrow \beta$ is a Δ -arrow. When our primary concern is the *size* of the G_α -orbit containing β , we will say that $\alpha \rightarrow \beta$ is an m -arrow, where m is this orbit size. Note that

$$m = |G_\alpha : G_\alpha \cap G_\beta| = |G_\beta : G_\alpha \cap G_\beta|,$$

where the second equality holds because $|G_\alpha| = |G_\beta|$. If $\alpha \rightarrow \beta$ is an m -arrow, therefore, then $\beta \rightarrow \alpha$ is also an m -arrow. This symmetry is also a consequence of the fact that $m = |\Delta|/|\Omega| = |\Delta'|/|\Omega|$, where Δ' is the orbital paired with Δ .

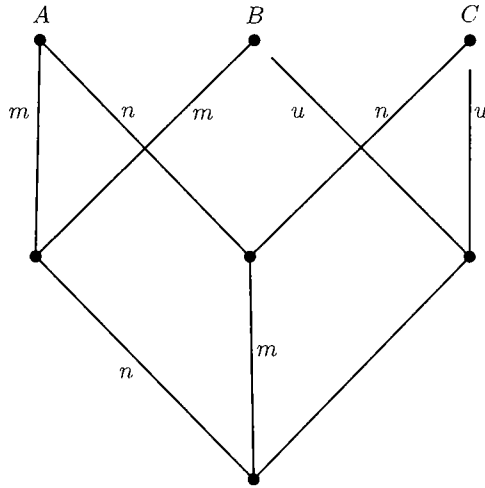
The first conclusion of the following lemma is needed for our proof of Theorem 8.38; the second and third will not be used until later.

8.39. Lemma. *Let G be a group acting transitively on Ω , and let $\alpha, \beta, \gamma \in \Omega$. Suppose that $\alpha \rightarrow \beta$ is an m -arrow and $\alpha \rightarrow \gamma$ is an n -arrow, where m*

and n are coprime, and let u be the integer associated with the arrows $\beta \rightarrow \gamma$ and $\gamma \rightarrow \beta$. The following then hold.

- (a) $u \geq n$.
- (b) u divides mn .
- (c) $G_\gamma G_\alpha \subseteq G_\gamma G_\beta$.

Note that the subgroup products in Lemma 8.39(c) are subsets of G , but they need not be subgroups. Before presenting the proof, we briefly review a few elementary facts. Let X and Y be subgroups of a finite group G . Then $|G| \geq |XY| = |X||Y|/|X \cap Y|$, and thus $|G : Y| \geq |X : X \cap Y|$. Also, $|G : X|$ and $|G : Y|$ divide $|G : X \cap Y|$, and so if these indices are coprime, then $|G : X||G : Y|$ divides $|G : X \cap Y|$. Then $|G : X||G : Y| \leq |G : X \cap Y|$, and we deduce that $|G| \leq |X||Y|/|X \cap Y|$. Equality thus holds in all of these inequalities, and in particular, $|G : Y| = |X : X \cap Y|$ and $|G : X||G : Y| = |G : X \cap Y|$. Also, $G = XY$ in this case.



Proof of Lemma 8.39. Write $A = G_\alpha$, $B = G_\beta$ and $C = G_\gamma$. Then $|A : A \cap B| = m$ and $|A : A \cap C| = n$, as indicated in the diagram. Since m and n are coprime, it follows that

$$\begin{aligned}
 n &= |A : A \cap C| = |A \cap B : (A \cap C) \cap (A \cap B)| \\
 &= |A \cap B : (A \cap B) \cap C| \\
 &\leq |B : B \cap C| \\
 &= u,
 \end{aligned}$$

proving (a). Also, since $|A| = |B|$, we see that $u = |B : B \cap C|$ divides

$$\begin{aligned} |B : A \cap B \cap C| &= |A : A \cap B \cap C| \\ &= |A : (A \cap B) \cap (A \cap C)| \\ &= |A : A \cap B| |A : A \cap C| \\ &= mn, \end{aligned}$$

and this establishes (b). Finally, $A = (A \cap C)(A \cap B)$, and thus

$$CA = C(A \cap C)(A \cap B) = C(A \cap B) \subseteq CB,$$

and this is (c). ■

Proof of Theorem 8.38. Let $\alpha \in \Omega$. Assume that $m \neq 1$, and choose an orbital Δ so that $|\Delta(\alpha)| = m$. Then Δ is not the diagonal, and hence by primitivity and Theorem 8.35, the corresponding orbital graph is connected. Every Δ -arrow is an m -arrow, however, and hence there is a path consisting of m -arrows from α to every other point in Ω . For $\delta \in \Omega$, let $d(\delta)$ denote the length of the shortest such path, and note that $d(\alpha) = 0$.

Now choose $\beta \in \Omega$ so that $\alpha \rightarrow \beta$ is an n -arrow. Of course, an m -arrow joins β to each point in $\Delta(\beta)$, and since $m \neq n$, we will have our desired contradiction when we prove that every arrow leaving β is an n -arrow, or equivalently, that every arrow arriving at β is an n -arrow. Now let $\gamma \in \Omega$. We show that the arrow $\gamma \rightarrow \beta$ is an n -arrow by induction on $d = d(\gamma)$, and that will complete the proof.

If $d = 0$, then $\gamma = \alpha$, and since $\alpha \rightarrow \beta$ is an n -arrow, there is nothing further to prove in this case. Now suppose that $d > 0$, so that there exists a point δ such that $\delta \rightarrow \gamma$ is an m -arrow and $d(\delta) = d - 1$. By the inductive hypothesis, $\delta \rightarrow \beta$ is an n -arrow, and since m and n are coprime, it follows by Lemma 8.37 that $\gamma \rightarrow \beta$ is a u -arrow, where $u \geq n$. But by hypothesis, n is the largest subdegree, and thus $u = n$ and the proof is complete. ■

The following theorem about multiple transitivity can also be proved by graph-theoretic techniques.

8.40. Theorem (Manning). *Suppose G is a group acting primitively on Ω , and let n be the largest subdegree. Assume that $n \geq 3$ and that a point stabilizer acts 2-transitively on some suborbit of size n . Then $n = |\Omega| - 1$, and G is 3-transitive on Ω .*

Proof. Let $\alpha \in \Omega$. By Lemma 8.2, we must show that G_α is 2-transitive on $\Omega - \{\alpha\}$. But G_α acts 2-transitively on an orbit of size n in Ω , so it suffices to show that $n = |\Omega| - 1$.

By hypothesis, there exists an orbital Δ such that G_α is 2-transitive on $\Delta(\alpha)$ and $|\Delta(\alpha)| = n$. Let X be an orbital (allowing $X = \Delta$) such that an X -arrow joins two distinct points of $\Delta(\alpha)$. Since G_α induces automorphisms of the orbital graph corresponding to X and G_α is 2-transitive on $\Delta(\alpha)$, it follows that every arrow joining two distinct points of $\Delta(\alpha)$ (in either direction) is an X -arrow. In particular the orbital X is self-paired.

Let $\beta \in \Delta(\alpha)$. Then $X(\beta)$ includes all of $\Delta(\alpha) - \{\beta\}$, and so $|X(\beta)| \geq n - 1$. Now $n - 1$ is relatively prime to n , and since $n - 1 > 1$ and n is the largest subdegree, it follows by Theorem 8.38 that $n - 1$ is not a subdegree. Thus $|X(\beta)| = n$, and so there is a unique point $\gamma \in X(\beta)$ with $\gamma \notin \Delta(\alpha)$.

Since G_α is 2-transitive on $\Delta(\alpha)$, we know that $(G_\alpha)_\beta$ acts transitively on the $n - 1$ points of $\Delta(\alpha) - \{\beta\} = X(\beta) - \{\gamma\}$. Also, since $(G_\alpha)_\beta$ is contained in G_β , it stabilizes the set $X(\beta)$, and it follows that $(G_\alpha)_\beta$ fixes γ . Then $(G_\alpha)_\beta \subseteq (G_\beta)_\gamma$, and since $(G_\alpha)_\beta$ is transitive on $X(\beta) - \{\gamma\}$, we see that G_β is 2-transitive on $X(\beta)$.

Now $n \geq 3$, so there are at least two points in the set $X(\beta) - \{\gamma\} = \Delta(\alpha) - \{\beta\}$, and since these points lie in $\Delta(\alpha)$, the arrow joining them must be an X -arrow. But G_β is 2-transitive on $X(\beta)$, and so by the reasoning we used before, every two distinct points in $X(\beta)$ are joined by an X -arrow. Furthermore, because G is transitive on Ω and defines automorphisms of the orbital graph corresponding to X , it follows that for an arbitrary point $\delta \in \Omega$, every two distinct points of $X(\delta)$ are joined by an X -arrow.

We now complete the proof by showing that $X(\beta) \cup \{\beta\} = \Omega$, so that $n = |\Omega| - 1$, as wanted. If this is false, then since the orbital graph corresponding to X is connected, there exists an X -arrow $\delta \rightarrow \epsilon$, where $\delta \in X(\beta) \cup \{\beta\}$ and $\epsilon \notin X(\beta) \cup \{\beta\}$. Then $\epsilon \in X(\delta)$, and since $\epsilon \notin X(\beta)$, we have $\delta \neq \beta$. Then $\delta \in X(\beta)$, and hence $\beta \in X(\delta)$ because X is self paired. Also, $\epsilon \neq \beta$, and since β and ϵ lie in $X(\delta)$, it follows by the previous paragraph that $\beta \rightarrow \epsilon$ is an X -arrow. This is a contradiction, however, since $e \notin X(\beta)$. ■

Even for imprimitive groups, these graph-theoretic techniques can be used to establish some necessary conditions on the set of subdegrees. To state our next result (which is a theorem of C. Praeger and the author) we introduce yet another graph. Given a set D of positive integers, the (undirected) **common-divisor graph** $\mathcal{G}(D)$ is constructed as follows. The vertex set of $\mathcal{G}(D)$ is D , and distinct integers $a, b \in D$ are joined by an edge precisely when they are not relatively prime. Note that if $1 \in D$, then no edge is incident with 1, and so $\{1\}$ is a connected component of $\mathcal{G}(D)$.

8.41. Theorem. *Let D be the set of distinct subdegrees for some transitive group action. Then the common-divisor graph $\mathcal{G}(D)$ has at most three connected components, including $\{1\}$.*

Thus, for example, the set $\{1, 2, 3, 4, 5\}$ cannot be the full set of subdegrees for a transitive group action because the corresponding common-divisor graph has four connected components: $\{1\}$, $\{2, 4\}$, $\{3\}$ and $\{5\}$.

Unfortunately, we need to introduce still more notation. Let G be transitive on Ω , and let m be a subdegree. Recall that if $\alpha, \beta \in \Omega$, we declared $\alpha \rightarrow \beta$ to be an m -arrow if β lies in a G_α -orbit of size m , or equivalently, if α lies in a G_β -orbit of size m . For $\alpha \in \Omega$, write $[\alpha]_m$ to denote the subset of Ω consisting of α and all points that can be reached from α along a path of m -arrows. In other words, $[\alpha]_m$ is the connected component containing α in what might be called the m -graph on Ω , defined by the m -arrows. Since each element of G carries m -arrows to m -arrows, we see that G acts as automorphisms of the m -graph, and thus it permutes the (necessarily disjoint) connected components. It follows that $[\alpha]_m$ is a block.

Now write

$$K_m(\alpha) = \langle G_\beta \mid \beta \in [\alpha]_m \rangle,$$

and observe that $G_\alpha \subseteq K_m(\alpha)$. It should be clear that if $g \in G$, we have $K_m(\alpha \cdot g) = K_m(\alpha)^g$, and thus since G acts transitively on Ω , the index $k_m = |K_m(\alpha) : G_\alpha|$ is independent of α . Of course, k_m does depend on m , and we stress that it is defined only when m is a subdegree.

If $\alpha \rightarrow \beta$ is a 1-arrow, then G_α fixes β , and thus $G_\alpha = G_\beta$. It follows that $K_1(\alpha) = G_\alpha$, and hence $k_1 = 1$. If $\alpha \rightarrow \beta$ is an m -arrow and $m > 1$, on the other hand, then G_α does not fix β , and thus $G_\alpha \neq G_\beta$ and $K_m(\alpha) \supseteq \langle G_\alpha, G_\beta \rangle > G_\alpha$. If $m > 1$, therefore, we have $k_m > 1$.

8.42. Theorem. *Let G be a group acting transitively on Ω . Suppose that $m < n$ are subdegrees, and assume that every subdegree is coprime to at least one of m or n . Then*

- (a) k_m divides k_n and
- (b) k_m divides n .

Proof. Fix $\gamma \in \Omega$ and consider the nonempty set S of all points $\alpha \in \Omega$ such that $\alpha \rightarrow \gamma$ is an n -arrow. If $\alpha \in S$ and $\alpha \rightarrow \beta$ is an m -arrow, we argue that $\beta \in S$. We know that $\beta \rightarrow \gamma$ is a u -arrow for some subdegree u , and our goal is to show that $u = n$. By Lemma 8.39(a), we have $u \geq n$, and if $u > n$, then of course also $u > m$, and so u cannot divide either n or m . But Lemma 8.39(b) tells us that u divides mn , and so if u is coprime to either m or n , it would have to divide the other, which is not the case. This u is not coprime to either m or n , which is contrary to the hypothesis. It follows that $u = n$, and thus $\beta \in S$, as claimed.

Now fix $\alpha \in S$. Since the set $[\alpha]_m$ is connected via m -arrows, it follows by the argument of the previous paragraph that $[\alpha]_m \subseteq S$. Then $[\alpha]_m \subseteq [\gamma]_n$,

and hence $K_m(\alpha) \subseteq K_n(\gamma)$. Since $|G_\alpha| = |G_\gamma|$, we have

$$\frac{k_n}{k_m} = \frac{|K_n(\gamma) : G_\gamma|}{|K_m(\alpha) : G_\alpha|} = |K_n(\gamma) : K_m(\alpha)|,$$

which is an integer. This establishes (a).

If $\alpha \rightarrow \beta$ is an m -arrow, we have $G_\gamma G_\alpha \subseteq G_\gamma G_\beta$ by Lemma 8.39(c). Since $\beta \rightarrow \alpha$ is also an m -arrow and we have shown that $\beta \in S$, we can interchange the roles of α and β to deduce the reverse containment, and thus $G_\gamma G_\alpha = G_\gamma G_\beta$. Since $[\alpha]_m$ is connected via m -arrows, this reasoning shows that for all $\delta \in [\alpha]_m$, the sets $G_\gamma G_\delta$ are equal, and thus $G_\gamma G_\alpha$ is invariant under right multiplication by each of the subgroups G_δ . It follows that $G_\gamma G_\alpha$ is invariant under right multiplication by $K_m(\alpha)$, which is the subgroup generated by these G_δ . Writing $K = K_m(\alpha)$ and noting that $G_\alpha \subseteq K$, we have

$$G_\gamma G_\alpha = G_\gamma G_\alpha K = G_\gamma K,$$

and thus

$$\frac{|G_\gamma||G_\alpha|}{|G_\gamma \cap G_\alpha|} = |G_\gamma G_\alpha| = |G_\gamma K| = \frac{|G_\gamma||K|}{|G_\gamma \cap K|}.$$

Then $|G_\alpha : G_\gamma \cap G_\alpha| = |K : G_\gamma \cap K|$, and this yields

$$\frac{n}{k_m} = \frac{|G_\alpha : G_\gamma \cap G_\alpha|}{|K : G_\alpha|} = \frac{|K : G_\gamma \cap K|}{|K : G_\alpha|} = \frac{|G_\alpha|}{|G_\gamma \cap K|} = |G_\gamma : G_\gamma \cap K|,$$

where the first equality holds because γ lies in a G_α -orbit of size n , and the last one holds because $|G_\alpha| = |G_\gamma|$. Since the quantity on the right is an integer, it follows that k_m divides n , and this completes the proof. ■

Theorem 8.41 follows easily from Theorem 8.42(b).

Proof of Theorem 8.41. Suppose that $u, v, w \in D$ lie in three different connected components of the common-divisor graph $\mathcal{G}(D)$. In particular u, v and w are distinct, and so we can assume that $u < v$ and $u < w$. Since u and v lie in different components, every subdegree is coprime to at least one of u or v , and so k_u divides v by Theorem 8.42(b). Similarly, k_u divides w , and since v and w are coprime, it follows that $k_u = 1$, and thus $u = 1$. This shows that there do not exist three connected components different from $\{1\}$ in $\mathcal{G}(D)$, and so there are at most three components in total. ■

Using Theorem 8.42(a) we can get additional information about the connected components of $\mathcal{G}(D)$.

8.43. Theorem. *Let D be the set of subdegrees for a transitive action, and assume that the common-divisor $\mathcal{G}(D)$ actually has three connected components: $\{1\}$, A and B . If B contains the largest subdegree n , then $a < b$ for all $a \in A$ and $b \in B$. Also, every two integers in B are joined by an edge.*

Proof. Let $a \in A$ and $b \in B$, and suppose that $a > b$. Then k_b divides a by 8.42(b), and also k_b divides k_a by 8.42(a). Furthermore, since $a \in A$ and $n \in B$, we have $a < n$, and thus k_a divides n by 8.42(b). Since k_b divides k_a , we see that k_b divides n , and since it also divides a and $k_b > 1$, it follows that a and n are not coprime. This is a contradiction, however, since a and n are in different connected components of the common-divisor graph.

If $a \in A$ and $u, v \in B$, then $a < u$ and $a < v$, and thus k_a divides both u and v . Since $k_a > 1$, we conclude that u and v are joined by an edge. ■

We saw previously that the set $\{1, 2, 3, 4, 5\}$ cannot be the full set of subdegrees of a transitive action because it does not satisfy the conclusion of Theorem 8.41. The connected components for the set $\{1, 2, 3, 4\}$, however, are $\{1\}$, $\{2, 4\}$ and $\{3\}$, and so this set is not eliminated by Theorem 8.41. By Theorem 8.43, however, $\{1, 2, 3, 4\}$ cannot be a subdegree set because in the notation of that theorem, $n = 4$, and thus $A = \{3\}$ and $B = \{2, 4\}$, and we do not have $a < b$ for all $a \in A$ and $b \in B$.

We close with an application of this material outside of the realm of transitive permutation groups.

8.44. Corollary. *Let A act on G via automorphisms, where A and G are finite groups, and let D be the set of sizes of the A -orbits on G . Then the common-divisor graph $\mathcal{G}(D)$ has at most three connected components including $\{1\}$. Also, if there are three components $\{1\}$, A and B , where B contains the largest member of D , then $a < b$ for all $a \in A$ and $b \in B$, and every two integers in B are joined by an edge.*

Proof. Let $\Gamma = G \rtimes A$, and view A and G as subgroups of Γ . Then Γ acts transitively on the set Ω of right cosets of A in Γ , and A is the stabilizer of the “point” $A \in \Omega$. The action of A on $\Omega - \{A\}$ is permutation isomorphic to the action of A on the nonidentity elements of G , and thus the action of A on Ω is permutation isomorphic to its original action on G . In particular, D is the set of subdegrees for the action of Γ on Ω , and hence Theorems 8.41 and 8.43 apply. ■

An important special case of Corollary 8.44 is where $A = G$, acting by conjugation. In that situation, D is just the set of class sizes of G , and it follows that the set of class sizes of an arbitrary finite group satisfies the conclusion of Corollary 8.44, and in particular, the common-divisor graph on this set has at most three connected components. Not surprisingly, more can be said in this case than seems to be available from the general theory we have presented.

Problems 8D

8D.1. Let $1 = m_1 \leq m_2 \leq \cdots \leq m_r$ be the subdegrees for a primitive action of rank r . If $m_2 = 2$, show that $m_i = 2$ for all $i \geq 2$.

8D.2. Show that a primitive permutation group of degree 8 must be doubly transitive.

8D.3. Let G be a transitive permutation group of rank r , and suppose that the largest subdegree is n . Prove that $|G|$ is bounded by some function of r and n .

8D.4. Let m be a subdegree for a transitive action of G on Ω , and let k_m be the integer defined just before Theorem 8.42.

- (a) Show that $k_m \geq m$.
- (b) If $k_m = m$ and $\alpha \rightarrow \beta$ is an m -arrow for $\alpha, \beta \in \Omega$, show that $G_\alpha G_\beta$ is a subgroup.
- (c) If $m > 1$ and G is primitive on Ω , show that $k_m > m$.

8D.5. Let G act transitively on Ω , and suppose the rank is 3. If the subdegrees are $1 < m < n$, where m and n are coprime, show that $m + 1$ must divide n .

Hint. Observe that k_m must divide $1 + m + n$.

8D.6. Let G be a primitive permutation group, and suppose that some prime number p is a subdegree. Prove that p^2 does not divide the order of a point stabilizer, and deduce that p^2 divides no subdegree.

Hint. If $X \subseteq Y$ and $|Y : X| = p$, prove that $\mathbf{O}^{p'}(X) \triangleleft Y$.

More on Subnormality

9A

In this chapter, we present a few more applications of subnormality theory, and also a pretty result within the theory for which no application seems to be known. We begin with a discussion of H. Bender's "generalized Fitting subgroup". This characteristic subgroup and its associated "components" have become standard tools in group theory, and they have played an essential role in the classification of simple groups.

Recall that the Fitting subgroup of a group G is the unique largest normal nilpotent subgroup. If G is solvable, it follows by Problem 3B.14 that the Fitting subgroup $\mathbf{F}(G)$ is large enough to contain its own centralizer in G . If we make the weaker assumption that G is p -solvable for some prime p , and we assume in addition that $\mathbf{O}_{p'}(G) = 1$, it is easy to see that $\mathbf{F}(G) = \mathbf{O}_p(G)$, and it follows by the Hall-Higman Lemma 1.2.3 that in this case too, $\mathbf{F}(G)$ contains its centralizer in G . But in general, of course, $\mathbf{F}(G)$ can fail to contain its centralizer. This certainly happens, for example, if G is a nonabelian simple group because in that case, $\mathbf{F}(G) = 1$.

In this section, we define the generalized Fitting subgroup $\mathbf{F}^*(G)$, and we prove that this characteristic subgroup always contains its centralizer in G . In general, $\mathbf{F}^*(G) \supseteq \mathbf{F}(G)$, and we shall see that in cases where the Fitting subgroup contains its centralizer, $\mathbf{F}^*(G) = \mathbf{F}(G)$. In other words, if no augmentation of the Fitting subgroup is necessary in order for it to contain its centralizer, then no augmentation occurs when we construct the generalized Fitting subgroup.

We begin work by recalling that a group G is said to be perfect if $G' = G$.

9.1. Lemma. *Let G be a group, and suppose that $G/\mathbf{Z}(G)$ is simple. Then $G/\mathbf{Z}(G)$ is nonabelian, and G' is perfect. Also $G'/\mathbf{Z}(G')$ is isomorphic to the simple group $G/\mathbf{Z}(G)$.*

Proof. Write $Z = \mathbf{Z}(G)$. If the simple group G/Z is abelian, it must be cyclic, and thus G is abelian and $Z = G$, which is a contradiction. Thus G/Z is a nonabelian simple group, as claimed. In particular, G is not solvable, and thus $G''' \neq 1$, so G'' is not abelian, and hence $G'' \not\subseteq Z$.

Now Z is a maximal normal subgroup of G and $G'' \not\subseteq Z$, and thus $G''Z > Z$, and we conclude that $G''Z = G$. Then $G/G'' = G''Z/G'' \cong Z/(Z \cap G'')$, which is abelian. Then G/G'' is abelian, and $G' \subseteq G''$. The reverse containment is obvious, so $G'' = G'$, and G' is perfect.

Finally, $G'/(Z \cap G') \cong G'Z/Z = G/Z$ is simple. It follows that $Z \cap G'$ is a maximal normal subgroup of G' , and since G' is nonabelian, we see that $Z \cap G'$ must be the full center of G' . Thus $G'/\mathbf{Z}(G') = G'/(Z \cap G') \cong G/Z$, and the proof is complete. ■

A group H is said to be **quasisimple** if $H/\mathbf{Z}(H)$ is simple and H is perfect. By Lemma 9.1, therefore, if $G/\mathbf{Z}(G)$ is simple, then G' is quasisimple. To produce examples of quasisimple groups, we observe first that all nonabelian simple groups are quasisimple. Also, the groups $SL(n, q)$ are quasisimple if $n \geq 3$ or $n = 2$ and $q > 3$, and most of these groups are not simple. (See Theorems 8.32 and 8.33.)

Of course, if G is quasisimple, there is a unique nonabelian simple group $G/\mathbf{Z}(G)$ associated with it. At first, it may seem that for each nonabelian finite simple group, there should be many (perhaps even infinitely many) associated quasisimple groups. In fact, there are only finitely many (and usually only a few). Although we will not present a proof here, it is a fact that for each nonabelian simple group S , there is a unique largest quasisimple group G (called the Schur representation group of S) such that $G/\mathbf{Z}(G) \cong S$. All of the quasisimple groups associated with S have the form G/Y , where G is the representation group of S and $Y \subseteq \mathbf{Z}(G)$. (The abelian group $\mathbf{Z}(G)$ is the Schur multiplier of S , and we refer the reader to a slightly more detailed discussion of Schur multipliers in Chapter 5.) For example, if S is the alternating group A_n with $n \geq 5$, then unless $n = 6$ or $n = 7$, the Schur multiplier has order 2, and so there are exactly two quasisimple groups associated with A_n in this case: the simple group A_n itself, and the corresponding representation group, which has order $2|A_n|$. If n is 6 or 7, the Schur multiplier of A_n is cyclic of order 6, and so there are exactly four associated quasisimple groups in these two cases, with orders $|A_n|$, $2|A_n|$, $3|A_n|$ and $6|A_n|$.

9.2. Lemma. *Let G be quasisimple. If N is a proper normal subgroup of G , then $N \subseteq \mathbf{Z}(G)$. Also, every nonidentity homomorphic image of G is quasisimple.*

Proof. Write $Z = \mathbf{Z}(G)$, so that Z is a maximal normal subgroup of G , and let $N \triangleleft G$ with $N < G$. If $N \not\subseteq Z$, then $NZ > Z$, and thus $NZ = G$ by the maximality of Z . Then $G/N = NZ/N \cong Z/(N \cap Z)$ is abelian, and so $G = G' \subseteq N < G$. This contradiction shows that $N \subseteq Z$.

To prove the second assertion, we show that $\overline{G} = G/N$ is quasisimple. We have $(\overline{G})' = \overline{G}' = \overline{G}$, and thus \overline{G} is perfect, as required. Also, since $N \subseteq Z$, we have $\overline{G}/\overline{Z} \cong G/Z$, which is simple and nonabelian. Since $\overline{Z} \subseteq \mathbf{Z}(\overline{G})$ and the factor group $\overline{G}/\overline{Z}$ is a nonabelian simple group, it follows that \overline{Z} must be the full center of \overline{G} , and this completes the proof. ■

A subnormal quasisimple subgroup of an arbitrary finite group G is called a **component** of G . (Of course, it can happen that G has no components; this is the situation if G is solvable, for example.) Observe that if H is a component of G , then it is also a component of every subgroup of G in which it happens to be contained.

9.3. Lemma. *Let N be a minimal normal subgroup of a finite group G , and suppose that H is a component of G with $H \not\subseteq N$. Then $[N, H] = 1$.*

Proof. First, $H \cap N < H$, and of course $H \cap N \triangleleft H$. By Lemma 9.2, therefore, $H \cap N \subseteq \mathbf{Z}(H)$. Now $H \triangleleft\triangleleft G$ and N is minimal normal in G , and so by Theorem 2.6, we know that $N \subseteq \mathbf{N}_G(H)$, and thus $[N, H] \subseteq H$. Also, $[N, H] \subseteq N$ since $N \triangleleft G$, and hence $[N, H] \subseteq H \cap N \subseteq \mathbf{Z}(H)$. Then $[N, H, H] = 1$ and $[H, N, H] = [N, H, H] = 1$, and so $[H, H, N] = 1$ by the three subgroups lemma. Since $H = H'$, we have $[H, N] = [H, H, N] = 1$, and the proof is complete. ■

9.4. Theorem. *Let H and K be distinct components of a finite group G . Then $[H, K] = 1$.*

Proof. We proceed by induction on $|G|$. If both H and K are contained in some proper subgroup X of G , then H and K are distinct components of X . By the inductive hypothesis applied in X , it follows that $[H, K] = 1$, as required, and so we can assume that no proper subgroup of G contains both H and K .

If G is simple, then since H and K are nontrivial and subnormal, we have $H = G = K$, which is not the case. Thus G is not simple, and since it is certainly nontrivial, G has a minimal normal subgroup N . Also, $N < G$, and thus N does not contain both H and K . If one of these components, say K , is contained in N , then $H \not\subseteq N$, and thus $[H, K] \subseteq [H, N] = 1$, by

Lemma 9.3, and we are done in this case. We can assume, therefore, that for every minimal normal subgroup N , we have $H \not\subseteq N$ and $K \not\subseteq N$.

Let $\overline{G} = G/N$, where N is minimal normal in G , and observe that \overline{H} and \overline{K} are nonidentity subnormal subgroups of \overline{G} . By Lemma 9.2, both \overline{H} and \overline{K} are quasisimple, and so they are components of \overline{G} . If $\overline{H} \neq \overline{K}$, then by the inductive hypothesis applied in the group \overline{G} , we have $[\overline{H}, \overline{K}] = 1$, and thus $[H, K] \subseteq N$. But $[N, H] = 1$ by Lemma 9.3, and thus $[H, K, H] = 1$ and $[K, H, H] = [H, K, H] = 1$. By the three subgroups lemma, therefore, we have $1 = [H, H, K] = [H, K]$, where the second equality holds because $H = H'$.

What remains is the case $\overline{H} = \overline{K}$, or equivalently, $HN = KN$, and we can assume that this equation holds for every choice of a minimal normal subgroup N of G . Since HN contains both H and K , it follows that $HN = G$. By Theorem 2.6, the minimal normal subgroup N normalizes H , and thus $H \triangleleft G$, and similarly $K \triangleleft G$, and hence $[H, K] \subseteq H \cap K$. If $[H, K] > 1$, we can choose our minimal normal subgroup N so that $N \subseteq H \cap K$, and thus $H = HN = KN = K$, and we have a contradiction. ■

It follows from Theorem 9.4 that the components of a finite group G normalize each other, and so each component is normal in the subgroup generated by all of them. This subgroup, denoted $\mathbf{E}(G)$, is called the **layer** of G . The layer of G is thus the product of the components of G , and of course, it is characteristic in G . (Of course, if G has no components, then $\mathbf{E}(G) = 1$.)

In order to discuss the properties of the layer, it is convenient to introduce another type of group that generalizes nonabelian simple groups. We say that a group G is **semisimple** if it is a product of nonabelian simple normal subgroups. (Unfortunately, not all authors agree on this definition, so readers should exercise caution.)

As the next lemma shows, semisimple groups are actually *direct* products of nonabelian simple groups.

9.5. Lemma. *Suppose that a finite group G is the product of the members of some collection \mathcal{X} of nonabelian simple normal subgroups. Then the product is direct, and \mathcal{X} is the set of all minimal normal subgroups of G .*

Proof. The members of \mathcal{X} are clearly minimal normal subgroups of G , and thus if $S \in \mathcal{X}$ and N is a minimal normal subgroup of G different from S , then $N \cap S = 1$, and hence S centralizes N . It follows that the product of all members of \mathcal{X} different from N centralizes N .

We can certainly assume that \mathcal{X} is nonempty. Let $T \in \mathcal{X}$, and let K be the product of all other members of \mathcal{X} , so that $TK = G$, and by the

result of the first paragraph, K centralizes T . Since T is nonabelian and simple, it has trivial center, and thus $T \cap K \subseteq \mathbf{Z}(T) = 1$, and it follows that $G = TK = T \times K$. Now K is the product of the members of the collection $\mathcal{X} - \{T\}$, so working by induction on $|\mathcal{X}|$, it follows that this product is direct, and thus $G = T \times K$ is the direct product of the members of \mathcal{X} .

Finally, if N is minimal normal in G and $N \notin \mathcal{X}$, then by the result of the first paragraph, N is centralized by $\prod \mathcal{X} = G$, and thus $N \subseteq \mathbf{Z}(G)$. But G is a direct product of groups having trivial centers, so $\mathbf{Z}(G) = 1$, and this contradiction shows that \mathcal{X} contains all minimal normal subgroups of G . ■

Next we show how semisimple groups arise naturally in finite group theory.

9.6. Lemma. *Let N be a minimal normal subgroup of a finite group G . Then either N is abelian or it is semisimple.*

Proof. Let S be a minimal normal subgroup of N . If S is abelian, then $S \subseteq \mathbf{F}(N)$, and thus $\mathbf{F}(N)$ is a nontrivial normal subgroup of G contained in N . Since N is minimal normal in G , we have $\mathbf{F}(N) = N$, and thus N is nilpotent. But then $\mathbf{Z}(N)$ is a nontrivial normal subgroup of G contained in N , and thus $\mathbf{Z}(N) = N$ and N is abelian.

We can now assume that S is nonabelian, and we argue that S is simple. If $K \triangleleft S$, then $K \triangleleft G$, and thus by Theorem 2.6, the minimal normal subgroup N of G normalizes K , and thus $K \triangleleft N$. But $K \subseteq S$ and S is minimal normal in N . Thus either $K = 1$ or $K = S$, and this shows that S is simple, as claimed.

We can now assume that S is a nonabelian simple group. Then each conjugate of S in G is a nonabelian simple group that is normal in N , and so the product S^G of these conjugates is semisimple. Also, $1 < S^G \triangleleft G$ and $S^G \subseteq N$, and it follows by the minimality of N that $S^G = N$. Thus N is semisimple, as wanted. ■

It follows by Lemma 9.5 that a nonabelian minimal normal subgroup of an arbitrary finite group must be a direct product of nonabelian simple groups.

We return now to the layer, $\mathbf{E}(G)$.

9.7. Theorem. *Let $E = \mathbf{E}(G)$, where G is a finite group, and write $Z = \mathbf{Z}(E)$. The following then hold.*

- (a) $E' = E$.
- (b) E/Z is semisimple.
- (c) $[E, M] = 1$ for every solvable normal subgroup M of G .

Proof. Let \mathcal{E} be the set of components of G , so that $E = \prod \mathcal{E}$. If $H \in \mathcal{E}$, then $H = H' \subseteq E'$, and thus E' contains all of the members of \mathcal{E} , and we have $E' \supseteq \prod \mathcal{E} = E$, proving (a).

Of course, $[\mathbf{Z}(H), H] = 1$, and if $K \in \mathcal{E}$ with $K \neq H$, then $[\mathbf{Z}(H), K] \subseteq [H, K] = 1$ by Theorem 9.4. Thus $\mathbf{Z}(H)$ centralizes all members of \mathcal{E} , and hence it is central in E . Then $\mathbf{Z}(H) \subseteq H \cap Z$, and since the reverse containment is clear, we have $\mathbf{Z}(H) = H \cap Z$ for all components H . Now write $\bar{E} = E/Z$. If $H \in \mathcal{E}$, then $\bar{H} \cong H/(H \cap Z) = H/\mathbf{Z}(H)$ is a nonabelian simple group. Also,

$$\bar{E} = \prod_{H \in \mathcal{E}} \bar{H}$$

is a product of nonabelian simple normal subgroups, and thus \bar{E} is semisimple, proving (b).

Finally, let $M \triangleleft G$ be solvable. Then $\overline{M \cap E}$ is a normal subgroup of the semisimple group \bar{E} . By Lemma 9.5, the minimal normal subgroups of \bar{E} are nonabelian simple groups, and in particular they are nonsolvable. It follows that the solvable normal subgroup $\overline{M \cap E}$ contains no minimal normal subgroup of \bar{E} , and thus $\overline{M \cap E} = 1$, and $M \cap E \subseteq Z$. Then $[M, E] \subseteq M \cap E \subseteq Z = \mathbf{Z}(E)$, and hence $[M, E, E] = 1$. Also, $[E, M, E] = [M, E, E] = 1$, and hence by the three subgroups lemma, $1 = [E, E, M] = [E, M]$, where the second equality follows by (a). This completes the proof. ■

Finally, we define the **generalized Fitting subgroup** of a finite group G by the formula $\mathbf{F}^*(G) = \mathbf{F}(G)\mathbf{E}(G)$.

9.8. Theorem. *For every finite group G , we have $\mathbf{F}^*(G) \supseteq \mathbf{C}_G(\mathbf{F}^*(G))$.*

Proof. Let $C = \mathbf{C}_G(\mathbf{F}^*(G))$, and write $Z = C \cap \mathbf{F}^*(G)$, so that our goal is to show that $Z = C$. If this is false, then $Z < C$, and since Z and G are normal in G , we can choose a minimal normal subgroup M/Z of G/Z with $M \subseteq C$. Since $Z \subseteq \mathbf{F}^*(G)$, we see that C centralizes Z , and since $M \subseteq C$, it follows that $Z \subseteq \mathbf{Z}(M)$.

Now M/Z is either abelian or semisimple by Lemma 9.6. If M/Z is abelian, then M is nilpotent, and so $M \subseteq \mathbf{F}(G) \subseteq \mathbf{F}^*(G)$, and thus $M \subseteq G \cap \mathbf{F}^*(G) = Z$, which is a contradiction. Thus M/Z is semisimple, and we let S/Z be a minimal normal subgroup of M/Z . Then S/Z is a nonabelian simple group by Lemma 9.5, and it follows that Z is the full center of S . Lemma 9.1 now applies, and we deduce that S' is quasisimple. Also, $S' \triangleleft G$, and so S' is a component of G , and $S' \subseteq \mathbf{E}(G) \subseteq \mathbf{F}^*(G)$. Then $S' \subseteq C \cap \mathbf{F}^*(G) = Z$, and thus S/Z is abelian. This is a contradiction, and the proof is complete. ■

9.9. Corollary. *Let G be a finite group. Then $\mathbf{F}^*(G) \supseteq \mathbf{F}(G)$, and equality holds if and only if $\mathbf{F}(G) \supseteq \mathbf{C}_G(\mathbf{F}(G))$.*

Proof. The containment is obvious. Also, since $\mathbf{F}^*(G)$ contains its centralizer in G , it follows that if $\mathbf{F}^*(G) = \mathbf{F}(G)$, then $\mathbf{F}(G)$ contains its centralizer.

Conversely, suppose that $\mathbf{F}(G) \supseteq \mathbf{C}_G(\mathbf{F}(G))$. Since $\mathbf{F}(G)$ is solvable, $\mathbf{E}(G) \subseteq \mathbf{C}_G(\mathbf{F}(G))$ by Theorem 9.7(c), and thus $\mathbf{E}(G) \subseteq \mathbf{F}(G)$, and hence $\mathbf{F}^*(G) = \mathbf{F}(G)\mathbf{E}(G) = \mathbf{F}(G)$, as required. ■

Problems 9A

9A.1. Suppose that $\mathbf{F}^*(G) \subseteq H \subseteq G$. Show that $\mathbf{E}(H) = \mathbf{E}(G)$.

9A.2. Show that the socle of an arbitrary finite group is the direct product of an abelian group with a semisimple group.

9A.3. Let $N \triangleleft G$, where G is semisimple. Show that N is the product of those minimal normal subgroups of G that it contains.

Hint. Write $G = U \times V$, where U is the product of the minimal normal subgroups of G that are contained in N . Show that $N \cap V = 1$.

9A.4. Let $E = \mathbf{E}(G)$ and suppose that $N \triangleleft E$. Show that $N = MY$, where M is the product of all components of G that are contained in N and $Y = M \cap \mathbf{Z}(E)$.

9A.5. Suppose that $H \triangleleft G$ and that C is a component of G not contained in H . Show that $[H, C] = 1$.

Hint. Use Problem 9A.4 to show that $[(H \cap E), C] = 1$, where $E = \mathbf{E}(H)$.

9A.6. Let $H \triangleleft G$, and suppose that $H \supseteq \mathbf{C}_G(H)$. Show that $H \supseteq \mathbf{E}(G)$.

9A.7. Let N be a nonabelian minimal normal subgroup of G , and observe that Lemmas 9.5 and 9.6 imply that N is a direct product of a collection \mathcal{X} of nonabelian simple groups. Prove that G acts transitively by conjugation on the set \mathcal{X} .

9A.8. A group G is **characteristically simple** if it is nontrivial and its only characteristic subgroups are 1 and G . If G is characteristically simple, show that G is a direct product of isomorphic simple groups.

Hint. Consider $G \rtimes \text{Aut}(G)$.

9B

If G is an arbitrary group, then $G/\mathbf{Z}(G)$ is naturally isomorphic to the group of inner automorphisms $\text{Inn}(G)$. If $\mathbf{Z}(G) = 1$, therefore, $G \cong \text{Inn}(G)$, and so we can identify G with $\text{Inn}(G)$ via the natural isomorphism, and this embeds G as a subgroup of $\text{Aut}(G)$. In fact, $\text{Inn}(G) \triangleleft \text{Aut}(G)$, and so a group with trivial center is naturally embedded as a normal subgroup of its automorphism group. (All of this is routine, but for completeness, the details are given in Lemma 9.11 below.) It is easy to show (and we will do this too in Lemma 9.11) that if $\mathbf{Z}(G) = 1$, then also $\mathbf{Z}(\text{Aut}(G)) = 1$, and so we can repeat the process and embed $\text{Aut}(G)$ as a normal subgroup of its automorphism group. Continuing like this, we obtain the **automorphism tower** associated with G :

$$G \triangleleft \text{Aut}(G) \triangleleft \text{Aut}(\text{Aut}(G)) \triangleleft \text{Aut}(\text{Aut}(\text{Aut}(G))) \triangleleft \cdots$$

One of the earliest applications of H. Wielandt's subnormality theory was his beautiful automorphism tower theorem, which asserts that the automorphism tower associated with a finite group having trivial center contains only finitely many different groups.

9.10. Theorem (Wielandt). *Let G be a finite group, and assume that $\mathbf{Z}(G) = 1$. Write $G_1 = G$, and for $i > 1$, let $G_i = \text{Aut}(G_{i-1})$. Then up to isomorphism, there are only finitely many different groups among the G_i .*

In this section, we present a proof of the automorphism tower theorem based on ideas of E. Schenkman and M. Pettet (and, of course, of Wielandt). Before we begin to develop the necessary theory, we mention that it does not seem to be known whether or not the hypothesis that G has trivial center is really necessary in Theorem 9.10. Without this assumption, we do not have natural embeddings of G_i in G_{i+1} , so there is no automorphism tower, but nevertheless, it might be true that there are just finitely many different groups G_i . For example, if G is dihedral of order 8, it happens that $\text{Aut}(G) \cong G$, and so there is only one group G_i in this case.

In the situation of Theorem 9.10, where $\mathbf{Z}(G) = 1$, we have remarked (but we have not yet proved) that the subgroups G_i all have trivial centers, and so there is a natural embedding $G_i \triangleleft G_{i+1}$. It follows that G is subnormal in each of the groups G_i , and this, of course, shows why subnormality theory is relevant here.

If we accept Wielandt's theorem for the moment, and we let G_r be the largest of the groups G_i , then clearly $G_r = G_{r+1}$. Since $G_{r+1} = \text{Aut}(G_r)$ and G_r is identified with $\text{Inn}(G_r)$, the equation $G_r = G_{r+1}$ tells us that every automorphism of G_r is inner. We mention that a group G with $\mathbf{Z}(G) = 1$ and

$\text{Aut}(G) = \text{Inn}(G)$ is said to be **complete**, and so it follows from Wielandt's theorem that every finite group with a trivial center can be subnormally embedded in a complete group.

Conversely, if one of the groups G_r in the automorphism tower of G is complete, then $G_r = \text{Inn}(G_r) = \text{Aut}(G_r) = G_{r+1}$, and hence $G_r = G_s$ for all subscripts $s \geq r$. In this situation, there are just finitely many groups appearing in the tower, and G_r is the largest of these. In other words, Theorem 9.10 is equivalent to the assertion that a complete group appears somewhere in the automorphism tower of an arbitrary finite group with trivial center. Our strategy of proof, however, will not be to show directly that some group in the automorphism tower is complete. We will show instead that if $\mathbf{Z}(G) = 1$, then there is some integer n , depending only on G , and such that $|G_i| \leq n$ for all terms G_i in the automorphism tower of G . This, of course, will show that there are only finitely many different groups G_i occurring, as required.

It is not completely trivial to find examples where $\mathbf{Z}(G) = 1$ and $\text{Aut}(G)$ is not complete. But if there were no such example, then automorphism towers would never contain more than two groups, and Wielandt's theorem would not be very interesting. Before we begin working toward a proof of the automorphism tower theorem, therefore, it seems appropriate to mention an example where there are three different groups in the automorphism tower. Let $G = S_3 \times S_3$, the direct product of two copies of the symmetric group of degree 3, and observe that $\mathbf{Z}(G) = 1$. Then $|G| = 36$, and one can compute that $|\text{Aut}(G)| = 72$ and $|\text{Aut}(\text{Aut}(G))| = 144$. This group of order 144, is complete; it can be constructed as the semidirect product of an elementary abelian group E of order 9, acted on by a semidihedral group of order 16, which is a full Sylow 2-subgroup of $\text{Aut}(E) \cong GL(2, 3)$.

Parts (a), (b) and (d) of the following establish the basic results about automorphisms to which we referred.

9.11. Lemma. *Let $A = \text{Aut}(G)$ and $I = \text{Inn}(G)$, where G is an arbitrary group, and for $g \in G$, write τ_g to denote the inner automorphism of G induced by g . The following then hold.*

- (a) *The map $g \mapsto \tau_g$ is a homomorphism from G onto I , with kernel $\mathbf{Z}(G)$.*
- (b) *$I \triangleleft A$.*
- (c) *If $\mathbf{Z}(G) = 1$, then $\mathbf{C}_A(I) = 1$.*
- (d) *If $\mathbf{Z}(G) = 1$, then $\mathbf{Z}(A) = 1$.*

Proof. Since $(x^g)^h = x^{(gh)}$ for elements $x, g, h \in G$, it is immediate that the map $g \mapsto \tau_g$ is a homomorphism from G onto I . Now $\tau_g = 1$ if and

only if $x^g = x$ for all $x \in G$, and this is true if and only if $g \in \mathbf{Z}(G)$. It follows that the kernel of the homomorphism $g \mapsto \tau_g$ is exactly $\mathbf{Z}(G)$, and this proves (a).

Now let $\alpha \in A$ and $g \in G$. Then for all $x \in G$, we have

$$(x)(\tau_g)^\alpha = (x)\alpha^{-1}\tau_g\alpha = (((x)\alpha^{-1})^g)\alpha = ((x)\alpha^{-1}\alpha)^{(g)\alpha} = (x)^{(g)\alpha},$$

and so $(\tau_g)^\alpha = \tau_{(g)\alpha}$, which lies in I . It follows that $I \triangleleft A$, proving (b).

Assume now that $\mathbf{Z}(G) = 1$, and suppose that $\alpha \in \mathbf{C}_A(I)$ in the previous calculation. If $g \in G$, we have

$$\tau_g = (\tau_g)^\alpha = \tau_{(g)\alpha},$$

and since the map $g \mapsto \tau_g$ is injective in this case, it follows that $g = (g)\alpha$. This holds for all $g \in G$, and so $\alpha = 1$. This establishes (c), and (d) is an immediate consequence. ■

Suppose that $\mathbf{Z}(G) = 1$, and let $G = G_1 \triangleleft G_2 \triangleleft G_3 \triangleleft \cdots$ be the automorphism tower of G . By Lemma 9.11(d), each of the groups G_i has a trivial center, and thus by 9.11(c), each of them has a trivial centralizer in its successor. The following result shows that in this situation, $\mathbf{C}_{G_i}(G) = 1$ for all i .

It is convenient now to change notation. We write S in place of G , so that we can use the symbol “ G ” to denote the largest group under consideration.

9.12. Lemma. *Let*

$$S = S_1 \triangleleft S_2 \triangleleft S_3 \triangleleft \cdots \triangleleft S_r = G,$$

where G is a group, and assume that $\mathbf{C}_{S_{i+1}}(S_i) = 1$ for all i with $1 \leq i < r$. Then $\mathbf{C}_G(S) = 1$.

Proof. The result is trivial if $r \leq 2$, and so we assume that $r > 2$, and we proceed by induction on r . Write $C = \mathbf{C}_G(S)$, and observe that $C \cap S_{r-1} = 1$ by the inductive hypothesis applied in the group S_{r-1} . Now S_2 normalizes S , and so S_2 normalizes G , and we have $[S_2, C] \subseteq C$. Also $S_2 \subseteq S_{r-1} \triangleleft G$, and thus $[S_2, C] \subseteq [S_{r-1}, G] \subseteq S_{r-1}$. Then $[S_2, C] \subseteq G \cap S_{r-1} = 1$, and so C centralizes S_2 . By the inductive hypothesis in G , with S_2 in place of S and $r - 1$ in place of r , we conclude that $G \subseteq \mathbf{C}_G(S_2) = 1$. ■

Now let G have trivial center, and suppose that its automorphism tower is $G = G_1 \triangleleft G_2 \triangleleft \cdots$. Recall that our goal is to show that there exists an integer n , depending only on G , and such that $|G_i| \leq n$ for all i . By Lemma 9.12, we know that $\mathbf{C}_{G_i}(G) = 1$, and thus the automorphism tower theorem will be an immediate consequence of the following result.

9.13. Theorem. *Let $S \triangleleft\triangleleft G$, where G is a finite group, and assume that $\mathbf{C}_G(S) = 1$. Then there exists an integer n depending only on the isomorphism type of S , and such that $|G| \leq n$.*

Our proof relies on two applications of the following easy lemma.

9.14. Lemma. *Let N be a normal subgroup of a finite group G , and suppose that $N \supseteq \mathbf{C}_G(N)$. Then $|G|$ divides $|\mathbf{Z}(N)||\text{Aut}(N)|$. In particular, $|G|$ divides $|N|!$.*

Proof. The conjugation action of G on N defines an isomorphism from $G/\mathbf{C}_G(N)$ into $\text{Aut}(N)$, and since $\mathbf{C}_G(N) = \mathbf{Z}(N)$, it follows that $|G|$ divides $|\mathbf{Z}(N)||\text{Aut}(N)|$, as claimed. Now $\text{Aut}(N)$ acts faithfully on the set of nonidentity elements of N , and so $|\text{Aut}(N)|$ divides $(|N| - 1)!$. Since $|\mathbf{Z}(N)|$ divides $|N|$, the final assertion follows. ■

Recall that in an arbitrary finite group S , there is a unique normal subgroup minimal with the property that the corresponding factor group is nilpotent. This subgroup, denoted S^∞ , is the final term of the lower central series of S . With this notation established, and before we plunge into the details, we can give a brief outline of the proof of Theorem 9.13

We show first that if S is an arbitrary subnormal subgroup of G , then the generalized Fitting subgroup $\mathbf{F}^*(G)$ normalizes S^∞ . If we can show that $\mathbf{N}_G(S^\infty)$ has bounded order, this will yield an upper bound on $|\mathbf{F}^*(G)|$, and since $\mathbf{F}^*(G)$ contains its centralizer in G , the result will follow by Lemma 9.14. In order to obtain an upper bound on $|\mathbf{N}_G(S^\infty)|$, we use the hypothesis that $\mathbf{C}_G(S) = 1$ to show that $\mathbf{C}_G(S^\infty) \subseteq S^\infty$. (This result of Schenkman seems to be the hardest step.) Then Lemma 9.14 yields $|\mathbf{N}_G(S^\infty)| \leq |\mathbf{Z}(S^\infty)||\text{Aut}(S^\infty)|$, and so this is an upper bound for $|\mathbf{F}^*(G)|$, as needed.

We begin work now with a number of preliminary results.

9.15. Lemma. *Let G be a finite group, and suppose that $G = SF$, where $S \triangleleft\triangleleft G$ and $F \triangleleft G$, and assume that F is nilpotent. Then $G^\infty = S^\infty$.*

Proof. Since there is nothing to prove if $S = G$, we can assume that $S < G$, and we proceed by induction on $|G|$. Let $S \subseteq M \triangleleft G$ with $M < G$. By Dedekind's lemma, $M = S(F \cap M)$, and so by the inductive hypothesis applied to M , with $F \cap M$ in place of F , we have $M^\infty = S^\infty$. It thus suffices to show that $M^\infty = G^\infty$.

Now $M^\infty \triangleleft G$, and we write $\overline{G} = G/M^\infty$. Observe that $G = MF$ since M contains S , and thus $\overline{G} = \overline{M}\overline{F}$ is a product of nilpotent normal subgroups, so it is contained in $\mathbf{F}(\overline{G})$, and hence is nilpotent. It follows that G/M^∞ is

nilpotent, and so $G^\infty \subseteq M^\infty$. The reverse containment is clear since M/G^∞ is nilpotent, and thus $M^\infty = G^\infty$. This completes the proof. ■

9.16. Corollary. *Let $S \triangleleft\triangleleft G$, where G is a finite group. Then $\mathbf{F}(G) \subseteq \mathbf{N}_G(S^\infty)$.*

Proof. By Lemma 9.15, we have $S^\infty = (\mathbf{F}(G)S)^\infty$, and since this subgroup is characteristic in $\mathbf{F}(G)S$, it is certainly normalized by $\mathbf{F}(G)$. ■

We must also show that the layer $\mathbf{E}(G)$ normalizes S^∞ for every subnormal subgroup S of G . Together with Corollary 9.16, this will show that $\mathbf{F}^*(G)$ normalizes S^∞ , as wanted.

9.17. Lemma. *Let $S \triangleleft\triangleleft G$, where G is a finite group and S is nonabelian and simple. Then the normal closure S^G is a minimal normal subgroup of G , and so $S \subseteq \text{Soc}(G)$.*

Proof. Recall that S^G is the subgroup generated by the members of the set $\mathcal{X} = \{S^g \mid g \in G\}$. Since the conjugates of S are simple, they are certainly quasisimple, and since they are subnormal, they are components. It follows by Theorem 9.4 that the members of \mathcal{X} normalize each other, and so $S^G = \prod \mathcal{X}$ and S^G is semisimple. To show that S^G is minimal normal in G , suppose that $1 < N \subseteq S^G$ with $N \triangleleft G$. Then N contains some minimal normal subgroup of S^G . By Lemma 9.5, this minimal normal subgroup is a member of \mathcal{X} , and thus N contains some conjugate of S . Since N is normal in G , it contains all conjugates of S , and it follows that $N = S^G$. This shows that S^G is minimal normal in G , as required. ■

9.18. Corollary. *Let $S \triangleleft\triangleleft G$, where G is a finite group. Then $\mathbf{E}(G)$ normalizes S^∞ .*

Proof. Let $Z = \mathbf{Z}(\mathbf{E}(G))$, and write $\overline{G} = G/Z$. Then $\overline{\mathbf{E}(G)}$ is semisimple, and by Lemma 9.17, each of its simple factors is contained in $\text{Soc}(\overline{G})$. Then $\overline{\mathbf{E}(G)} \subseteq \text{Soc}(\overline{G})$, and we conclude by Theorem 2.6 that $\overline{\mathbf{E}(G)}$ normalizes the subnormal subgroup $\overline{S} = \overline{SZ}$. It follows that $\mathbf{E}(G)$ normalizes SZ , and so it normalizes $(SZ)^\infty = S^\infty$, where the equality follows by Lemma 9.15. ■

Our next goal will be to show that if $S \triangleleft\triangleleft G$, and we assume in addition that $\mathbf{C}_G(S) = 1$, then $\mathbf{C}_G(S^\infty) \subseteq S^\infty$. This is a result of Schenkman, and we begin with the following easy fact, which can also be obtained as a consequence of Problem 1D.15.

9.19. Lemma. *Let $N \triangleleft G$, where G is a finite group, and suppose that $N \subseteq \Phi(G)$, the Frattini subgroup. If G/N is nilpotent, then G is nilpotent.*

Proof. By Theorem 1.26, it suffices to show that $M \triangleleft G$, where M is an arbitrary maximal subgroup of G . But $M \supseteq \Phi(G) \supseteq N$, so by the correspondence theorem, M/N is maximal in the nilpotent group G/N . It follows that $M/N \triangleleft G/N$, and thus $M \triangleleft G$. ■

9.20. Lemma. *Let N be a normal subgroup of a finite group G , and assume that G/N is nilpotent. Then there exists a nilpotent subgroup $H \subseteq G$ such that $NH = G$.*

Proof. Since obviously, $NG = G$, the set of subgroups $H \subseteq G$ such that $NH = G$ is nonempty, and we show that a minimal member of this set must be nilpotent. We argue that if H is minimal such that $NH = G$, then $N \cap H \subseteq \Phi(H)$. Otherwise, there exists a maximal subgroup M of H such that $N \cap H \not\subseteq M$, and thus since $N \cap H \triangleleft H$, we see that $(N \cap H)M$ is a subgroup of H that properly contains M . Then $(N \cap H)M = H$, and we have $G = NH = N(N \cap H)M = NM$. This contradicts the minimality of H , and thus $N \cap H \subseteq \Phi(H)$, as claimed. Now $H/(N \cap H) \cong NH/N = G/N$, and this is a nilpotent group. It follows that by Lemma 9.19 that H is nilpotent. ■

9.21. Theorem (Schenkman). *Let $S \triangleleft\triangleleft G$, where G is a finite group and $C_G(S) = 1$. Then $C_G(S^\infty) \subseteq S^\infty$.*

First, we prove the case of Schenkman's theorem where $S = G$.

9.22. Theorem. *Let G be a finite group, and suppose that $\mathbf{Z}(G) = 1$. Then $C_G(G^\infty) \subseteq G^\infty$.*

Proof. Let $C = C_G(G^\infty)$, and note that $C \triangleleft G$. We argue that if $H \subseteq G$ is a nilpotent subgroup such that $G^\infty H = G$, then $C \cap H = 1$. Otherwise, $G \cap H$ is a nontrivial normal subgroup of the nilpotent group H , and so it contains a nontrivial central subgroup Z of H . Then $H \subseteq C_G(Z)$, and since $Z \subseteq C$, also $G^\infty \subseteq C_G(Z)$. Then $G = G^\infty H \subseteq C_G(Z)$, and this is a contradiction, since $\mathbf{Z}(G) = 1$ by hypothesis.

We will show that it is possible to choose a nilpotent subgroup $H \subseteq G$ such that $G^\infty H = G$ and so that in addition, $G = (G \cap G^\infty)(G \cap H)$. Since $G \cap H = 1$ by the result of the previous paragraph, it will follow that $C = C \cap G^\infty$, and this will complete the proof.

By Lemma 9.20, there exists a nilpotent subgroup $K \subseteq G$ such that $G^\infty K = G$. Writing $T = CK$, we argue that $T^\infty \subseteq C \cap G^\infty$. To see this, observe first that each term of the lower central series of T is contained in the corresponding term of the lower central series of G , and thus $T^\infty \subseteq G^\infty$. Also, $T/G = CK/C$ is nilpotent because K is nilpotent, and thus $T^\infty \subseteq G$, and this shows that $T^\infty \subseteq C \cap G^\infty$, as wanted. By Lemma 9.20 applied

in the group T , therefore, we can find a nilpotent subgroup H such that $T = (G \cap G^\infty)H$. Since $C \cap G^\infty \subseteq C \subseteq T$, Dedekind's lemma yields $C = (C \cap G^\infty)(C \cap H)$. Also,

$$G^\infty H = G^\infty (G \cap G^\infty)H = G^\infty T \supseteq G^\infty K = G,$$

and thus $G^\infty H = G$, so H has the desired properties. This completes the proof. ■

Proof of Theorem 9.21. Let $G = \mathbf{C}_G(S^\infty)$, and observe that $C \cap S \subseteq S^\infty$ by Theorem 9.22. Since S normalizes S^∞ , it also normalizes C , and hence SC is a group, and it is no loss to assume that $SC = G$. We proceed by induction on $|G|$.

Suppose that $S \subseteq H < G$. Then $S \triangleleft H$, and since $\mathbf{C}_H(S) = 1$ and $H < G$, the inductive hypothesis yields $H \cap G \subseteq S^\infty$. By Dedekind's lemma, however, $H = S(H \cap G) \subseteq SS^\infty = S$, and so $H = S$. It follows that there are no subgroups H with $S < H < G$, and since $S \triangleleft G$, we conclude that $S \triangleleft G$, and G/S has no nonidentity proper subgroups. Then G/S is cyclic, and since $C/(C \cap S^\infty) = G/(C \cap S) \cong SC/S = G/S$, we see that $C/(C \cap S^\infty)$ is cyclic. But $G \cap S^\infty \subseteq \mathbf{Z}(G)$, and we deduce that G is abelian. Then $G^\infty = (SG)^\infty = S^\infty$ by Lemma 9.15.

Now $\mathbf{Z}(G) \subseteq \mathbf{C}_G(S) = 1$, so we can apply Theorem 9.22 to G to deduce that $\mathbf{C}_G(G^\infty) \subseteq G^\infty$. Since $G^\infty = S^\infty$, the result follows. ■

We can now prove Theorem 9.13, thereby completing the proof of Wielandt's automorphism tower theorem.

Proof of Theorem 9.13. Since $S^\infty \triangleleft \mathbf{N}_G(S^\infty)$ and Theorem 9.21 guarantees that S^∞ contains its centralizer in $\mathbf{N}_G(S^\infty)$, it follows by Lemma 9.14 that

$$|\mathbf{N}_G(S^\infty)| \leq |\mathbf{Z}(S^\infty)||\text{Aut}(S^\infty)|.$$

Now $\mathbf{F}^*(G) = \mathbf{F}(G)\mathbf{E}(G)$, and each factor is contained in $\mathbf{N}_G(S^\infty)$ by Corollaries 9.16 and 9.18, and thus $|\mathbf{F}^*(G)| \leq |\mathbf{Z}(S^\infty)||\text{Aut}(S^\infty)|$. Since $\mathbf{F}^*(G)$ contains its centralizer in G by Theorem 9.8, Lemma 9.14 yields

$$|G| \leq |\mathbf{F}^*(G)|! \leq (|\mathbf{Z}(S^\infty)||\text{Aut}(S^\infty)|)!,$$

and thus $|G|$ is bounded in terms of S , as required. ■

Problems 9B

9B.1. Let $S \triangleleft G$, where S is complete. Show that $G = S \times T$ for some subgroup T .

9B.2. Suppose that $\mathbf{Z}(G) = 1$, and let $G = G_1 \triangleleft G_2 \triangleleft \cdots$ be the automorphism tower of G . If $G \triangleleft G_i$, show that $i \leq 2$.

9B.3. If G is semisimple, show that $\text{Aut}(G)$ is complete, and thus the automorphism tower for G contains at most two different groups.

9B.4. Let G be dihedral of order $2n$, where n is odd. Observe that $\mathbf{Z}(G) = 1$, and show that the automorphism tower of G contains at most two different groups.

9B.5. Let $G = AB$, where $A, B \triangleleft\triangleleft G$. Show that $G^\infty = A^\infty B^\infty$.

Hint. First do the case where both A and B are normal, and then work by induction on $|G|$.

9C

We mentioned the Sims conjecture in Chapter 8. Restated in purely group-theoretic language, this conjecture asserts that there exists some function $f(m)$, defined for positive integers m , such that the following holds. Let $H \subseteq G$ be a maximal subgroup, and assume that $\text{core}_G(H) = 1$. (In this situation, the subgroup H is said to be **corefree**.) Let $g \in G$ with $g \notin H$, and let $m = |H : H \cap H^g|$. Then $|H| \leq f(m)$.

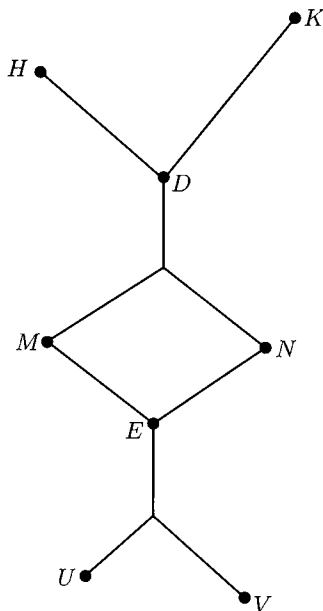
It is a triviality that if $m = 1$ then $|H| = 1$, and if $m = 2$, then $|H| = 2$. If $m = 3$, then $|H|$ is a divisor of 48 by a 1967 theorem of C. Sims, but no general bounds for integers m exceeding 3 were known to exist until 1983, when P. Cameron, C. Praeger, J. Saxl and G. Seitz proved the full conjecture in a paper relying on the classification of simple groups.

There is, however, an elementary argument that seems to come close to proving the Sims conjecture, and which is the starting point of the paper by Cameron *et al.* This result, proved by Thompson and simplified by Wielandt, is an application of subnormality theory, and it is the subject of this section. Thompson proved that there is a function $t(m)$ such that in the context of the Sims conjecture, $|H : \mathbf{O}_p(H)| \leq t(m)$ for some prime p . In other words, although Thompson did not show that $|H|$ is bounded, he did prove that if H is unboundedly large, then it must be “mostly” a p -group.

9.23. Theorem (Thompson). *Let H be a corefree maximal subgroup of a finite group G . Let $g \in G - H$, and write $m = |H : H \cap H^g|$. Then for some prime p , we have $|H : \mathbf{O}_p(H)| \leq ((m!)^2)!$.*

We prove the following somewhat more general form of this theorem. (The diagram should help the reader to keep track of the many subgroups involved.)

9.24. Theorem. *Let H and K be distinct subgroups of a finite group G . Write $D = H \cap K$, and assume that no nonidentity subgroup of D is normal in any subgroup of G that properly contains either H or K . Let $M = \text{core}_H(D)$ and $N = \text{core}_K(D)$, and let $E = M \cap N$. Then at least one of the subgroups $U = \text{core}_H(E)$ and $V = \text{core}_K(E)$ is a p -group for some prime p .*



Under the hypotheses of Theorem 9.24, let $a = |H : D|$ and $b = |K : D|$. By the $n!$ -theorem, we have $|H : M| \leq a!$ and $|K : N| \leq b!$. It follows that $|D : E| \leq |D : M||D : N| \leq (a-1)!(b-1)!$, and thus $|H : E| \leq a!b!$ and $|K : E| \leq a!b!$. By the $n!$ -theorem once again, $|H : U| \leq (a!b!)!$ and $|K : V| \leq (a!b!)!$. Theorem 9.24 asserts that one of U or V is a p -group for some prime p , and since $U \triangleleft H$ and $V \triangleleft K$, we deduce that either $|H : \mathbf{O}_p(H)| \leq (a!b!)!$ or $|K : \mathbf{O}_p(K)| \leq (a!b!)!$.

To see why Theorem 9.23 follows from Theorem 9.24, assume the hypotheses of 9.23, and suppose that $H > 1$. Since H is maximal and has trivial core, we have $H = \mathbf{N}_G(H)$, and thus g does not normalize H , and we can take $K = H^g$, so that H and K are distinct. By the maximality of H again, the only subgroup of G that properly contains either H or K is G itself, and since H is corefree, no nonidentity subgroup of $D = H \cap K$ is normal in G . The hypotheses of Theorem 9.24 are thus satisfied, and in the above notation, $a = m = b$. Since H and K are isomorphic, it

does not matter which of U or V is a p -group since in either case, we have $|H : \mathbf{O}_p(H)| \leq ((m!)^2)!$, as asserted by Theorem 9.23.

9.25. Lemma. *Let $H \subseteq G$, where G is a finite group and $\mathbf{F}(G) = 1$, and assume that $\mathbf{E}(G) \subseteq H$. Then $\mathbf{E}(G) = \mathbf{E}(H)$.*

Proof. Since $\mathbf{E}(G) \subseteq H$, each component of G is contained in H , and so the components of G are components of H , and we have $\mathbf{E}(G) \subseteq \mathbf{E}(H)$. To establish equality, it suffices to show that all components of H are contained in $\mathbf{E}(G)$, so suppose that U is a component of H and $U \not\subseteq \mathbf{E}(G)$. Then certainly U is not a component of G , and so each component of G is a component of H different from U . By Theorem 9.4, distinct components of H centralize each other, and it follows that U centralizes all of the components of G , and thus $U \subseteq \mathbf{C}_G(\mathbf{E}(G))$. But $\mathbf{F}(G) = 1$, so $\mathbf{F}^*(G) = \mathbf{E}(G)$, and thus $U \subseteq \mathbf{C}_G(\mathbf{F}^*(G)) \subseteq \mathbf{F}^*(G) = \mathbf{E}(G)$, and this is a contradiction. ■

Next, we prove an analog of Lemma 9.15.

9.26. Lemma. *Let $G = SP$, where G is a finite group, and where $S \triangleleft\triangleleft G$ and $P \triangleleft G$, and P is a p -group for some prime p . Then $\mathbf{O}^p(G) = \mathbf{O}^p(S)$.*

Proof. If $S = G$, there is nothing to prove, so we can assume $S < G$, and we choose M with $S \subseteq M \triangleleft G$ and $M < G$. Then $M = S(M \cap P)$, and so working by induction on $|G|$ and applying the inductive hypothesis to M , we have $\mathbf{O}^p(M) = \mathbf{O}^p(S)$, and it suffices to show that $\mathbf{O}^p(M) = \mathbf{O}^p(G)$.

Now $\mathbf{O}^p(M) \triangleleft G$, and we write $\overline{G} = G/\mathbf{O}^p(M)$. Since $S \subseteq M$, we have $G = MP$, and thus $\overline{G} = \overline{M}\overline{P}$, which is a p -group. It follows that $\mathbf{O}^p(G) \subseteq \mathbf{O}^p(M)$. The reverse containment holds because $M/\mathbf{O}^p(G)$ is a p -group, and this completes the proof. ■

9.27. Corollary. *Let G be a finite group. Suppose that $S \triangleleft\triangleleft G$, and let $P \triangleleft G$ be a p -group. Then P normalizes $\mathbf{O}^p(S)$.*

Proof. By Lemma 9.26, we have $\mathbf{O}^p(S) = \mathbf{O}^p(SP)$. This subgroup is characteristic in SP , so it is normalized by P . ■

Proof of Theorem 9.24. Since $V \triangleleft K$, we have $V \triangleleft M \triangleleft H$, so $V \triangleleft\triangleleft H$, and similarly, $U \triangleleft\triangleleft K$. Also, we can certainly assume that $H > 1$, and since $\mathbf{F}^*(H) \supseteq \mathbf{C}_G(\mathbf{F}^*(H))$, it follows that $\mathbf{F}^*(H) > 1$, and thus either $\mathbf{F}(H) > 1$ or $\mathbf{E}(H) > 1$, and similarly, we can assume that either $\mathbf{F}(K) > 1$ or $\mathbf{E}(K) > 1$.

Suppose first that $\mathbf{F}(H) = 1$ and $\mathbf{F}(K) = 1$, so that $\mathbf{E}(H) > 1$ and $\mathbf{E}(K) > 1$. We show in this case that either $U = 1$ or $V = 1$, and so U or V is a p -group, as required. Assuming that $U > 1$ and $V > 1$, we see that neither U nor V is nilpotent, and thus U^∞ and V^∞ are nontrivial subgroups of D ,

normal in H and K , respectively. Then $H = \mathbf{N}_G(U^\infty)$ and $K = \mathbf{N}_G(V^\infty)$ because nontrivial subgroups of D cannot be normal in subgroups properly containing H or K . Since $V \triangleleft\triangleleft H$, it follows by Corollary 9.18 that $\mathbf{E}(H) \subseteq \mathbf{N}_G(V^\infty) = K$. Then $\mathbf{E}(H) \subseteq D$, and Lemma 9.25 yields $\mathbf{E}(H) = \mathbf{E}(D)$. Similarly, $\mathbf{E}(K) = \mathbf{E}(D)$, and thus $\mathbf{E}(H) = \mathbf{E}(K)$ is a nontrivial subgroup of D , normal in both H and K . Then $H = \mathbf{N}_G(\mathbf{E}(H)) = \mathbf{N}_G(\mathbf{E}(K)) = K$, which is a contradiction.

We can now assume that either $\mathbf{F}(H) > 1$ or $\mathbf{F}(K) > 1$, and by symmetry, we can suppose that $\mathbf{F}(H) > 1$. Then $\mathbf{O}_p(H) > 1$ for some prime p , and we write $P = \mathbf{O}_p(H)$. Let $X = \mathbf{O}^p(U)$ and $Y = \mathbf{O}^p(V)$, and observe that it suffices to show that at least one of X or Y is trivial. Assuming that $X > 1$ and $Y > 1$, we have $H = \mathbf{N}_G(X)$ and $K = \mathbf{N}_G(Y)$, and we work to derive a contradiction.

Since $V \triangleleft\triangleleft H$ and $P \triangleleft H$, it follows by Corollary 9.27 that P normalizes $Y = \mathbf{O}^p(V)$, and so $P \subseteq \mathbf{N}_G(Y) = K$. Then $P \subseteq D$, and in fact, $P \triangleleft D$ since $P \triangleleft H$.

Now let $k \in K$. We have $U \triangleleft H$, so $U \triangleleft N$, and hence $U^k \triangleleft N^k = N$. Since $N \triangleleft D$, we have $U^k \triangleleft\triangleleft D$, and by Corollary 9.27 applied in the group D , it follows that P normalizes $\mathbf{O}^p(U^k) = X^k$. Then $P \subseteq \mathbf{N}_G(X^k) = (\mathbf{N}_G(X))^k = H^k$, and we deduce that $P^{k^{-1}} \subseteq H$. Since also $P^{k^{-1}} \subseteq K$, we have $P^{k^{-1}} \subseteq D$, and thus $P \subseteq D^k$ for all $k \in K$. Then $P \subseteq \text{core}_K(D) = N$, and so $P \triangleleft N$, and we have $\mathbf{O}_p(H) = P \subseteq \mathbf{O}_p(N) \subseteq \mathbf{O}_p(K)$, where the last containment follows since $N \triangleleft K$.

Now $1 < P \subseteq \mathbf{O}_p(K)$, and so we can interchange the roles of H and K in the previous argument. We deduce that $\mathbf{O}_p(K) \subseteq \mathbf{O}_p(H)$, and so equality holds. Thus P is a subgroup of D normal in both H and K , and since $P > 1$, we have $H = \mathbf{N}_G(P) = K$, which is a contradiction. This completes the proof. ■

Problems 9C

9C.1. Suppose that both H and K are subnormal in G in Theorem 9.24. Prove that either $U = 1$ or $V = 1$.

Hint. Otherwise, $\mathbf{O}_p(G) > 1$ for some prime p . Show that $\mathbf{Z}(\mathbf{O}_p(G)) \subseteq H$ by considering separately the cases where U is or is not a p -group.

9C.2. Let $G = AB$, where $A, B \triangleleft\triangleleft G$. Show that $\mathbf{O}^p(G) = \mathbf{O}^p(A)\mathbf{O}^p(B)$.

Hint. As with Problem 9B.5, first handle the case where A and B are both normal, and then proceed by induction on $|G|$.

9C.3. Let $G = \langle A, B \rangle$, where $A, B \triangleleft G$, and suppose that $|A : A'|$ and $|B : B'|$ are coprime. Prove that $G = AB$ by assuming that G is a minimal counterexample to this assertion and carrying out the following steps.

- (a) Let N be minimal normal in G . Show that $ANB = G$.
- (b) Show that $(N \cap A)(N \cap B)$ is normalized by both A and B .
- (c) Show that $N \cap A = 1 = N \cap B$, and N has prime order, say p .
- (d) Now assume that p does not divide $|B : B'|$. Use the previous problem to show that $\mathbf{O}^p(G) = \mathbf{O}^p(A)B$.
- (e) Derive a contradiction using the fact that $A\mathbf{O}^p(G)$ is a group.

9D

In the previous three sections, we presented applications of subnormality to general group theory. We close this chapter with a pretty result of D. Bartels that lies within subnormality theory itself. Our goal is to prove an analog for subnormal subgroups of the obvious fact that if $X \subseteq G$, then the normal closure of X in G , which by definition is the unique smallest normal subgroup of G that contains X , is exactly the subgroup generated by all of the conjugates of X in G .

First, we observe that for an arbitrary subgroup $X \subseteq G$, there is a unique smallest subnormal subgroup of G that contains X . This subgroup is the **subnormal closure** of X in G , and it exists because intersections of subnormal subgroups are subnormal, and so the intersection of all subnormal subgroups containing X has the desired properties. By analogy with the normal closure X^G , the notation X^{**G} is sometimes used to denote the subnormal closure of X in G . Observe that we always have $X^{**G} \subseteq X^G$, and $X \triangleleft G$ if and only if $X = X^{**G}$. Since X^G is generated by all of the G -conjugates of X and $X^{**G} \subseteq X^G$, it is perhaps natural to guess that the subnormal closure X^{**G} is generated by *some* of the conjugates of X .

Given $X, Y \subseteq G$, we say that X and Y are **strongly conjugate** in G if X and Y are conjugate in the group $\langle X, Y \rangle$, or equivalently, X and Y are conjugate in every subgroup of G that contains both of them. (But note that strong conjugacy is *not* usually an equivalence relation; it is reflexive and symmetric, but in general, it is not transitive.) We saw in Problem 2A.10 that $X \triangleleft G$ if and only if X has no strong conjugates in G distinct from itself, and this suggests that perhaps in general, the subnormal closure of X is the subgroup generated by all of the strong conjugates of X in G . This is, in fact true, and it is easy to see that Problem 2A.10 is an immediate consequence.

9.28. Theorem (Bartels). *Let $X \subseteq G$, where G is a finite group. Then*

$$X^{\bullet\bullet G} = \langle Y \mid Y \text{ is strongly conjugate to } X \rangle.$$

We write $X^{(G)}$ to denote the subgroup generated by all of the strong conjugates of X in G . Thus Bartels' theorem asserts that $X^{(G)} = X^{\bullet\bullet G}$, and so once we establish the theorem, the notation $X^{(G)}$ becomes superfluous.

We begin work by noting some elementary properties of the subgroup $X^{(G)}$. First, observe that if X and Y are strongly conjugate in G and $g \in G$, then X^g and Y^g are strongly conjugate, and thus $(X^{(G)})^g = (X^g)^{(G)}$. The following lemma establishes a few slightly less trivial properties.

9.29. Lemma. *Let $X \subseteq G$, where G is a finite group.*

- (a) *If $X \subseteq S \triangleleft G$, then $X^{(G)} \subseteq S$.*
- (b) *If $Y \subseteq X \subseteq G$, then $Y^{(G)} \subseteq X^{(G)}$.*
- (c) *If $X \subseteq K \subseteq G$, then $X^{(K)} \subseteq X^{(G)}$.*
- (d) *If $X^{(G)} \subseteq K \subseteq G$, then $X^{(K)} = X^{(G)}$, and in particular, if $K = X^{(G)}$, then $K = X^{(K)}$.*

Proof. We prove (a) by induction on $|G|$. Let $X \subseteq S \triangleleft G$, and observe that since there is nothing to prove if $S = G$, we can assume that $S < G$. Then there exists a subgroup $M \triangleleft G$ with $S \subseteq M < G$, and all conjugates of X in G are contained in M . The strong conjugates of X in G , therefore, are exactly the strong conjugates of X in M , and thus $X^{(G)} = X^{(M)} \subseteq S$, where the containment holds by the inductive hypothesis applied in the group M .

For (b), let $Y \subseteq X$, and suppose that Y and Z are strongly conjugate in G . Then $Z = Y^g \subseteq X^g$ for some element $g \in \langle Y, Z \rangle \subseteq \langle X, X^g \rangle$, and thus X and X^g are strongly conjugate in G , and $X^g \subseteq X^{(G)}$. Therefore $Z = Y^g \subseteq X^g \subseteq X^{(G)}$, and since $Y^{(G)}$ is generated by all such subgroups Z , it follows that $Y^{(G)} \subseteq X^{(G)}$, as wanted.

Now let $X \subseteq K \subseteq G$. The strong conjugates of X in K are exactly those strong conjugates of X in G that are contained in K . Thus $X^{(K)} \subseteq X^{(G)}$, and this proves (c). If $X^{(G)} \subseteq K$, then K contains all strong conjugates of X in G , so $X^{(K)} = X^{(G)}$, proving (d). ■

The following is somewhat less routine.

9.30. Lemma. *Let N be a normal subgroup of a finite group G , and write $\overline{G} = G/N$. Then $\overline{X^{(G)}} = \overline{X}^{(\overline{G})}$ for all subgroups X of G .*

Proof. It is clear that the canonical homomorphism $g \mapsto \overline{g}$ maps the set of conjugates of X in G onto the set of conjugates of \overline{X} in \overline{G} . We will show

that the set of strong conjugates of X in G maps onto the set of strong conjugates of \overline{X} in \overline{G} , and the result then follows.

First, suppose that Y is strongly conjugate to X in G . Then $Y = X^g$ for some element $g \in \langle X, Y \rangle$, and we have $\overline{Y} = (\overline{X})^{\overline{g}}$ and $\overline{g} \in \langle \overline{X}, \overline{Y} \rangle = \langle \overline{X}, \overline{Y} \rangle$. Thus \overline{Y} is strongly conjugate to \overline{X} in \overline{G} , as required.

Conversely, consider a strong conjugate of \overline{X} in \overline{G} . Since this subgroup is conjugate to \overline{X} , it has the form \overline{Y} for some (not uniquely determined) conjugate Y of X in G . Let \mathcal{Y} be the set of all conjugates Y of X in G such that \overline{Y} is the given strong conjugate of \overline{X} , and observe that it suffices to show that some member of \mathcal{Y} is strongly conjugate to X .

Choose $Y \in \mathcal{Y}$ so that the subgroup $\langle X, Y \rangle$ has the smallest possible order. Since \overline{X} and \overline{Y} are strongly conjugate, they are conjugate in $\langle \overline{X}, \overline{Y} \rangle = \langle \overline{X}, Y \rangle$, and thus there is some element $g \in \langle X, Y \rangle$ such that $\overline{Y} = (\overline{X})^{\overline{g}}$. Then $NX^g = (NX)^g = NY$, and thus $X^g \in \mathcal{Y}$. Also, by the choice of Y , we have $|\langle X, X^g \rangle| \geq |\langle X, Y \rangle|$. Since $g \in \langle X, Y \rangle$, however, we see that $X^g \subseteq \langle X, Y \rangle$, and thus $\langle X, X^g \rangle \subseteq \langle X, Y \rangle$. We deduce that $\langle X, X^g \rangle = \langle X, Y \rangle$, and since g is an element of this subgroup, X^g is strongly conjugate to X . But $X^g \in \mathcal{Y}$, and so the proof is complete. ■

We also need the following easy general fact.

9.31. Lemma. *Let $S \triangleleft G$ and $P \in \text{Syl}_p(G)$, where G is a finite group. Then $P \cap S \in \text{Syl}_p(S)$.*

Proof. If $S = G$, there is nothing to prove, so we assume that $S < G$, and we work by induction on $|G|$. Let $S \subseteq M < G$ with $M \triangleleft G$, and observe that $|M : M \cap P| = |PM : P|$ is coprime to p . Then $M \cap P \in \text{Syl}_p(M)$, and thus $S \cap P = S \cap (M \cap P) \in \text{Syl}_p(S)$ by the inductive hypothesis. ■

Proof of Theorem 9.28. By Lemma 9.29(a), we have $X^{(G)} \subseteq X^{**G}$. We must prove the reverse containment, and for this purpose, it suffices to show that $X^{(G)} \triangleleft G$. Suppose that this is false, and assume that $|G|$ is as small as possible for a counterexample. Also, assume that $|X|$ is as small as possible among subgroups $X \subseteq G$ such that $X^{(G)}$ is not subnormal. Note that $X^{(G)} < G$, and hence $X < G$. We proceed in a number of steps.

Step 1. Suppose that Y and Z are conjugates of X and that $Y^{(H)} = Z^{(H)}$ for some subgroup H containing Y and Z . Then $Y^{(G)} = Z^{(G)}$.

Proof. Write $K = Y^{(G)}$, and let $U = Y^{(H)}$, so that also $U = Z^{(H)}$. We have $U = Z^{(U)}$ and $K = Y^{(K)}$ by Lemma 9.29(d), and $U = Y^{(H)} \subseteq Y^{(G)} = K$ by 9.29(c). Since Y is conjugate to X , we see that $K = Y^{(G)}$ is conjugate to

$X^{(G)} < G$, and thus $K < G$. Thus $Z^{(K)} \triangleleft K$ by the minimality of G , and we have

$$Y \subseteq U = Z^{(U)} \subseteq Z^{(K)} \triangleleft K,$$

where the second containment follows from 9.29(c) because $U \subseteq K$. Then $Y^{(K)} \subseteq Z^{(K)}$ by 9.29(a), and we have

$$Y^{(G)} = K = Y^{(K)} \subseteq Z^{(K)} \subseteq Z^{(G)},$$

where the last containment follows by yet another application of 9.29(c). We have just proved that $Y^{(G)} \subseteq Z^{(G)}$, and since the reverse containment follows symmetrically, we have equality, as required.

Step 2. X is a p -group for some prime p .

Proof. Otherwise, since X is certainly generated by its Sylow subgroups, it follows that $X = \langle Y \mid Y < X \rangle$. Now write $U = \langle Y^{(G)} \mid Y < X \rangle$ and observe that since $Y \subseteq Y^{(G)}$, we have $X \subseteq U$, and also, $U \subseteq X^{(G)}$ by 9.29(b). By the minimality of X , each of the subgroups $Y^{(G)}$ for $Y < X$ is subnormal in G , and thus $U \triangleleft G$. But $X \subseteq U$, so we have $X^{(G)} \subseteq U$ by 9.29(a). Since we established the reverse containment previously, we have $X^{(G)} = U \triangleleft G$. This is a contradiction, and we conclude that X is a p -group, as claimed.

Step 3. Let $Y \subseteq H < G$, where Y is conjugate to X , and let $P \in \text{Syl}_p(H)$. Then there exists $Z \subseteq P$ with Z conjugate to X , such that $Y^{(G)} = Z^{(G)}$.

Proof. Since $H < G$, we have $Y^{(H)} \triangleleft H$, and thus $P \cap Y^{(H)} \in \text{Syl}_p(Y^{(H)})$ by Lemma 9.31. As Y is a p -subgroup of $Y^{(H)}$, we can write $Y^h \subseteq P \cap Y^{(H)}$ for some element $h \in Y^{(H)}$. Writing $Z = Y^h$, we have $Z \subseteq P$ and

$$Z^{(H)} = (Y^h)^{(H)} = (Y^{(H)})^h = Y^{(H)},$$

and thus $Y^{(G)} = Z^{(G)}$ by Step 1.

Step 4. Let M be a maximal subgroup of G containing X , and let $P \in \text{Syl}_p(M)$. Then $P \in \text{Syl}_p(G)$, and M is the unique maximal subgroup of G containing P .

Proof. For subgroups $H \subseteq G$, write $\mathcal{K}(H)$ to denote the set of all subgroups of the form $Y^{(G)}$, where $Y \subseteq H$ and Y is conjugate to X in G . If $h \in H$ and $Y \subseteq H$ is conjugate to X , then $(Y^{(G)})^h = (Y^h)^{(G)}$, and it follows that H acts by conjugation on the set $\mathcal{K}(H)$. Also, $\mathbf{Z}(H)$ is contained in the kernel of this action.

Now G acts transitively on $\mathcal{K}(G)$, and M stabilizes (setwise) the subset $\mathcal{K}(M) \subseteq \mathcal{K}(G)$. The full stabilizer in G of $\mathcal{K}(M)$ is thus a subgroup of G

that contains the maximal subgroup M , so it is either M itself, or else it is all of G .

Suppose first that G stabilizes $\mathcal{K}(M)$. Since G acts transitively on $\mathcal{K}(G)$, it follows that $\mathcal{K}(M) = \mathcal{K}(G)$. By Step 3, we also have $\mathcal{K}(M) = \mathcal{K}(P)$, and thus $\mathcal{K}(G) = \mathcal{K}(P)$. Now $\mathbf{Z}(P)$ acts trivially on $\mathcal{K}(P) = \mathcal{K}(G)$, and it follows that the action of G on $\mathcal{K}(G)$ has a nontrivial kernel K . Of course, $K \triangleleft G$, and we write $\overline{G} = G/K$, so that $|\overline{G}| < |G|$. By Lemma 9.30 and the minimality of G , we have

$$\overline{X^{(G)}} = \overline{X}^{(\overline{G})} \triangleleft\triangleleft \overline{G},$$

and so $KX^{(G)} \triangleleft\triangleleft G$. Also, $X^{(G)} \triangleleft KX^{(G)}$ because K stabilizes $X^{(G)}$, and thus $X^{(G)} \triangleleft\triangleleft G$. This is a contradiction, and it follows that G does not stabilize $\mathcal{K}(M)$.

Then M is the full stabilizer of $\mathcal{K}(M) = \mathcal{K}(P)$, and this set is stabilized by $\mathbf{N}_G(P)$. Thus $\mathbf{N}_G(P) \subseteq M$, and since $P \in \text{Syl}_p(M)$, it follows easily that P must be a full Sylow p -subgroup of G , as required. Also if $P \subseteq N$, where N is maximal in G , then $P \in \text{Syl}_p(N)$, and similar reasoning shows that N is the full stabilizer of $\mathcal{K}(P)$. Thus $N = M$, as wanted.

Step 5. X is contained in a unique maximal subgroup of G .

Proof. Otherwise, let M and N be distinct maximal subgroups such that $X \subseteq M \cap N$, and let $X \subseteq S \in \text{Syl}_p(M \cap N)$. Choose M and N so that $|S|$ is as large as possible. If $S \in \text{Syl}_p(G)$, then Step 4 yields $M = N$, which is a contradiction. Also, observe that $X \triangleleft\triangleleft S$, so if $S \triangleleft G$, then $X \triangleleft\triangleleft G$. Then $X^{(G)} = X$ by 9.29(a), so $X^{(G)}$ is subnormal, which is a contradiction. Thus $\mathbf{N}_G(S)$ is proper, and so it is contained in some maximal subgroup R of G .

Now let $S \subseteq P \in \text{Syl}_p(M)$ and $S \subseteq Q \in \text{Syl}_p(N)$, and note that P and Q are full Sylow p -subgroups of G by Step 4. Then $S < P$ and $S < Q$, and so $R \cap P > S$ and $R \cap Q > S$, and thus Sylow p -subgroups of $M \cap R$ and $N \cap R$ are larger than S . By the choice of M and N , it follows that $M = R = N$, which is a contradiction.

Step 6. We have a contradiction.

Proof. We have $X^{(G)} \subseteq X^G \triangleleft G$, and thus $X^{(G)}$ cannot be subnormal in X^G , and it follows by the minimality of $|G|$ that $X^G = G$.

Let M be the unique maximal subgroup of G that contains X . Then $X^G \not\subseteq M$, so some conjugate Y of X is not contained in M . If $\langle X, Y \rangle$ is contained in some maximal subgroup N , then $X \subseteq N$, and so $N = M$, and this is a contradiction because $Y \not\subseteq M$. Thus $\langle X, Y \rangle = G$ and Y is strongly conjugate to X . Then $G = \langle X, Y \rangle \subseteq X^{(G)} < G$, which is a contradiction. ■

Problems 9D

9D.1. Just as subnormal closures exist, so too do subnormal cores. Prove that if $X \subseteq G$, then there exists a unique largest subgroup of X that is subnormal in G . Show that this **subnormal core** of X in G is normal in X .

9D.2. Let $X \subseteq G$. Prove that the intersection L of all strong conjugates of X in G is normal in X and subnormal in G .

Hint. Show that $L^{(G)} \subseteq X$.

9D.3. Prove that the subnormal core of X in G is not necessarily the intersection of any collection of conjugates of X .

Hint. Let $G = S_4$, the symmetric group of degree 4, and take X to be cyclic of order 4.

9D.4. A converse of Lemma 9.31 asserts that if $S \subseteq G$, and for all primes p and all Sylow p -subgroups P of G , the intersection $P \cap S$ is a Sylow p -subgroup of S , then S is subnormal in G . Suppose that $S \subseteq G$ yields a counterexample to this assertion with $|S| + |G|$ as small as possible. Show that G and S are nonabelian simple groups. In particular, this converse of 9.31 holds if S is solvable.

Hint. Consider a minimal normal subgroup of G .

Note. This converse to Lemma 9.31 was conjectured by O. Kegel. It was eventually proved by P. Kleidman using the classification of simple groups.

More Transfer Theory

10A

We begin with a brief review of some material from Chapter 5. Let P be a Sylow p -subgroup of a finite group G , and let $v : G \rightarrow P/P'$ be the transfer homomorphism. We proved that $\ker(v)$ is the subgroup $A^p(G)$, which, by definition, is the smallest normal subgroup of G such that the corresponding factor group is an abelian p -group. One goal of transfer theory is to find a relatively small subgroup N , where $P \subseteq N \subseteq G$, and such that $G/A^p(G) \cong N/A^p(N)$. (In other words, we want N to control p -transfer in G .) If this happens, it might allow us to prove that G is nonsimple by studying the smaller group N and showing that N has a nontrivial abelian p -factor group. Then $A^p(N) < N$, and thus by control of p -transfer, $A^p(G) < G$. Assuming that G does not have order p , therefore, it cannot be simple.

A natural candidate for control of p -transfer is the Sylow normalizer $N = N_G(P)$, but this does not always work. For example, $N_G(P)$ fails to control p -transfer if G is the alternating group A_6 , with $p = 2$. There $N_G(P) = P$, and $A^p(P)$ has index 4 in P , but G is simple.

If the Sylow subgroup P is abelian, we proved in Chapter 5 that $N_G(P)$ actually does control p -transfer in G . This was done in two steps: first, Lemma 5.12 shows that $N = N_G(P)$ controls G -fusion in P , which means that whenever two elements of P are conjugate in G , they are already conjugate in N , and then by Corollary 5.22, we know that whenever $P \subseteq N \subseteq G$ and N controls G -fusion in P , it also controls p -transfer in G .

If the Sylow p -subgroup P is nonabelian, the Sylow normalizer usually does not control fusion in P . Nevertheless, even in this case, there are situations where $N_G(P)$ can be proved to control p -transfer. The main result

of this section is a powerful theorem of this type due to T. Yoshida. It strengthens earlier results of P. Hall and H. Wielandt, and it guarantees that the Sylow normalizer controls p -transfer if the Sylow subgroup P is not too far from being abelian. More precisely, $\mathbf{N}_G(P)$ controls p -transfer if the nilpotence class of P is less than the prime p . (If $p = 2$, this corollary of Yoshida's theorem tells us nothing new, although the theorem itself has content for all primes.) Our proof was inspired by Yoshida's original character-theoretic argument, but it is more elementary than his, and it does not rely on character theory.

For a given prime p , the key to Yoshida's theorem is the wreath product $W = C_p \wr C_p$, where C_p is the cyclic group of order p . The group W can be defined as a semidirect product $A \rtimes U$, where A is the direct product of p copies of C_p and $U \cong C_p$. Of course, to construct the semidirect product W , we need a specific action of U on A , and to describe it we write

$$A = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_p \rangle,$$

and $U = \langle u \rangle$, and we let U act on A by setting $(a_i)^u = a_{i+1}$ for $1 \leq i < p$, and $(a_p)^u = a_1$. Following the usual custom, we view A and U as subgroups of $W = C_p \wr C_p$.

Before stating Yoshida's theorem, we make a few routine observations about the group $W = C_p \wr C_p$. First, we see that the subgroup A of W satisfies $|W : A| = p$ and $|A| = p^p$. Also, A is elementary abelian, which means that it is abelian and that $x^p = 1$ for all elements $x \in A$. Furthermore, A is generated by the subset $\{a_1, a_2, \dots, a_p\}$, which consists of p elements that are conjugate in W , and whose product is not the identity.

In general, if P is an arbitrary nonabelian group having an abelian subgroup A of prime index p , then $\mathbf{Z}(P) \subseteq A$. (Otherwise $A\mathbf{Z}(P) > A$ and thus $P = A\mathbf{Z}(P)$ is abelian.) In this situation, if $a \in A - \mathbf{Z}(P)$, then $\mathbf{C}_P(a) = A$, and hence the conjugacy class of a in P has size p . Applying this to the group W , we conclude that the generating elements a_i form a full conjugacy class of W .

10.1. Theorem (Yoshida). *Let $P \in \text{Syl}_p(G)$ and $N = \mathbf{N}_G(P)$, where G is a finite group. Then N controls p -transfer in G unless P has a homomorphic image isomorphic to $C_p \wr C_p$.*

10.2. Corollary. *Let $P \in \text{Syl}_p(G)$ and $N = \mathbf{N}_G(P)$, where G is a finite group. If the nilpotence class of P is less than p , then N controls p -transfer in G .*

Proof. By Lemma 10.3, below, the group $C_p \wr C_p$ has nilpotence class p , so it cannot be a homomorphic image of a p -group with class less than p . The result is now immediate from Theorem 10.1. ■

Of course, we can also conclude that $N_G(P)$ controls p -transfer in G if the Sylow p -subgroup P satisfies one of the several other conditions on a p -group that are sufficient to guarantee that $C_p \wr C_p$ is not a homomorphic image. For example, if P has exponent p , then $C_p \wr C_p$ cannot be a homomorphic image because $C_p \wr C_p$ contains an element of order p^2 , namely ua_1 . More generally, if for every two elements $x, y \in P$, there exists an element c in the derived subgroup of $\langle x, y \rangle$ such that $(xy)^p = x^p y^p c^p$, then $C_p \wr C_p$ cannot be a homomorphic image. (A p -group that satisfies this condition is said to be **regular**. There is a fairly extensive theory of regular p -groups, which we will not discuss here, but we mention that the theorem of Hall and Wielandt that is generalized by Yoshida's theorem asserts that the normalizer of a regular Sylow p -subgroup controls p -transfer.)

To apply Yoshida's theorem, one must show that $C_p \wr C_p$ is not a homomorphic image of some given p -group, but to prove the theorem, we need conditions on a p -group sufficient to guarantee that $C_p \wr C_p$ actually is a homomorphic image. That is the goal of the next few results.

Since the group $W = C_p \wr C_p$ satisfies the hypotheses of the following lemma with $t = p$, the lemma implies that $|Z(W)| = p$, that W' is elementary abelian of order p^{p-1} , and that the nilpotence class of W is p .

10.3. Lemma. *Let P be a p -group, and let $A \triangleleft P$, where $|P : A| = p$, and A is elementary abelian of order p^t for some integer $t \geq 2$. Suppose that A is generated by the elements of some conjugacy class of P . The following then hold.*

- (a) $|Z(P)| = p$.
- (b) P' is elementary abelian of order p^{t-1} .
- (c) The nilpotence class of P is t .

Proof. Let K be a conjugacy class of P that generates A . Since $|A| = p^t > p$ and A is elementary abelian, we see that A is not cyclic, and thus the class K contains more than one element. It follows that P is nonabelian, and hence $Z(P) \subseteq A$.

Now $P' \subseteq A$ because P/A has order p , and so if $a \in K$, we have $\langle a \rangle P' \subseteq A$. Since $\langle a \rangle P'$ contains P' , it is a normal subgroup of P , and hence it contains the entire conjugacy class K . But K generates A , and thus we have $\langle a \rangle P' = A$, and since $|\langle a \rangle| = p$, it follows that $|A : P'| \leq p$. This yields $p \geq |A|/|P'| = |Z(P)| \geq p$, where the equality follows by Lemma 4.6, and the final inequality holds since P is a p -group. Thus $|Z(P)| = p = |A : P'|$, and (a) and (b) are proved. Also P has nilpotence class t by Theorem 4.7, and thus (c) holds. ■

By writing the group operation in an elementary abelian p -group as addition, the group can be viewed as a vector space over the field $\mathbb{Z}/p\mathbb{Z}$ of order p , and this enables us to use linear-algebra techniques. In particular, since the subgroups of an elementary abelian group are exactly the subspaces, and since every subspace of a finite dimensional vector space is a direct summand, it follows that if X is an arbitrary subgroup of an elementary abelian group E , then $E = X \times Y$ for some subgroup $Y \subseteq E$. This observation and some other standard facts from linear algebra will be used in the proof of the next result.

Recall that the elements a_i of the group $W = C_p \wr C_p$, form a conjugacy class of W contained in the elementary abelian subgroup A , and that the product of these elements is not the identity. Together with the fact that $|\mathbf{Z}(W)| = p$ established in Lemma 10.3, this provides a useful way to recognize $C_p \wr C_p$, and this is the content of the following.

10.4. Theorem. *Let P be a p -group, and let $A \triangleleft P$, where A is elementary abelian and $|P : A| = p$. Suppose that $|\mathbf{Z}(P)| = p$, and assume that the product of the elements of some noncentral conjugacy class of P contained in A is not the identity. Then $P \cong C_p \wr C_p$.*

Proof. Since P has a noncentral conjugacy class, it is nonabelian, and thus $\mathbf{Z}(P) \subseteq A$. But A is elementary abelian, and so we can write $A = \mathbf{Z}(P) \times B$, for some subgroup $B \subseteq A$. Then $|A : B| = |\mathbf{Z}(P)| = p$, and we have $|P : B| = p^2$. Also, since $B \cap \mathbf{Z}(P) = 1$ and every nonidentity normal subgroup of P meets $\mathbf{Z}(P)$ nontrivially, it follows that $\text{core}_P(B) = 1$, and thus the right-multiplication action of P on the p^2 right cosets of B in P is faithful. We conclude that P is isomorphic to a subgroup of the symmetric group S_{p^2} .

Let $a \in K$, where K is a noncentral class of P such that $K \subseteq A$ and the product of the elements of K is not the identity. Choose $u \in P - A$, and let $T : A \rightarrow A$ be the map $x \mapsto x^u$. Then T^p is the identity map on A since $u^p \in A$ and A is abelian. Also, $K = \{aT^i \mid 0 \leq i < p\}$.

Now view A as a vector space over the field F of order p . Then T is a linear operator on A and $T^p = I$, the identity operator on A . Since F has characteristic p , we have $(T - I)^p = T^p - I = 0$, and we let k be the smallest positive integer such that $(T - I)^k = 0$. Then $k \leq p$, and

$$A > A(T - I) > A(T - I)^2 > \cdots > A(T - I)^{k-1} > A(T - I)^k = 0,$$

and it follows that $\dim(A) \geq k$.

Next, we compute with polynomials over the field F to obtain

$$(X - 1)^{p-1} = \frac{(X - 1)^p}{X - 1} = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{p-1}.$$

If $k < p$, then

$$0 = (T - I)^{p-1} = I + T + T^2 + \cdots + T^{p-1},$$

and thus

$$a + aT + aT^2 + \cdots + aT^{p-1} = 0.$$

Since $K = \{aT^i \mid 0 \leq i \leq p-1\}$, it follows that (in the original multiplicative notation) the product of the elements of K is the identity, and this is a contradiction. We conclude that $k = p$, and thus $\dim(A) \geq p$ and $|A| \geq p^p$, and we have $|P| \geq p^{p+1}$.

By the result of the first paragraph, P is isomorphic to a subgroup of the symmetric group S_{p^2} . Since the full p -part of $(p^2)!$ is p^{p+1} and we have shown that $|P| \geq p^{p+1}$, it follows that in fact, P is isomorphic to a Sylow p -subgroup of S_{p^2} . But all Sylow p -subgroups of this group are isomorphic, and so P is uniquely determined up to isomorphism. The group $C_p \wr C_p$ satisfies the hypotheses of the theorem, however, and it follows that $P \cong C_p \wr C_p$, as required. ■

We mention that the proof of Theorem 10.4 yields another way to think about the group $C_p \wr C_p$: it is a Sylow p -subgroup of the symmetric group S_{p^2} . We shall not need this observation, however.

10.5. Corollary. *Let P be a p -group, and let $A \triangleleft P$, where A is an elementary abelian subgroup of index p . Let $a \in A - \mathbf{Z}(P)$, and assume that the product of the p elements in the conjugacy class of a in P is not the identity. Then $C_p \wr C_p$ is a homomorphic image of P .*

Proof. Let $\{a_i \mid 1 \leq i \leq p\}$ be the conjugacy class of a , and write $b = a_1 a_2 \cdots a_p$, so that $b \neq 1$ by assumption, and $\langle b \rangle \subseteq \mathbf{Z}(P)$. If $|\mathbf{Z}(P)| = p$, then $P \cong C_p \wr C_p$ by Theorem 10.4, and there is nothing more to prove. We can thus assume that $\mathbf{Z}(P) > \langle b \rangle$, and we let $z \in \mathbf{Z}(P) - \langle b \rangle$. Then $z \in A$, and thus $Z = \langle z \rangle$ has order p , and $b \notin Z$.

Now consider the group $\bar{P} = P/Z$. Since $b \notin Z$, we see that \bar{b} is nontrivial, and it is the product of the conjugate elements \bar{a}_i for $1 \leq i \leq p$. If these factors were all equal, then since $(a_1)^p = 1$, we would have $\bar{b} = (\bar{a}_1)^p = 1$, which is not the case.

Since $\{\bar{a}_i\}$ is a conjugacy class of \bar{P} contained in \bar{A} , and its cardinality exceeds 1, it follows that this class has size p . The elements \bar{a}_i are thus distinct, and the product of these elements is the nonidentity element \bar{b} . Thus \bar{P} satisfies the hypotheses of the lemma, and working by induction on P , we can conclude that $C_p \wr C_p$ is a homomorphic image of \bar{P} . It is thus also a homomorphic image of P , as required. ■

We also need to consider p -groups for which we are not given an elementary abelian subgroup of index p . This is where transfer becomes relevant, and so perhaps a brief review of some basic transfer theory would be useful.

Let $H \subseteq G$ have finite index, and let T be a right transversal for H in G . (Recall that this means that exactly one member of T lies in each right coset of H in G .) If $t \in T$ and $g \in G$, we write $t \cdot g$ to denote the unique element of T lying in the coset Htg . This defines an action of G on T , and we see that $tg(t \cdot g)^{-1}$ lies in H . A pretransfer map $V : G \rightarrow H$ is defined by the formula

$$V(g) = \prod_{t \in T} tg(t \cdot g)^{-1},$$

where the factors are multiplied according to some fixed, but arbitrary linear order on the elements of T . In general, the map V depends on the transversal T and the particular order on the elements of T , but the composition of V with the canonical homomorphism $H \rightarrow H/H'$ is the uniquely defined transfer homomorphism $v : G \rightarrow H/H'$, which is independent of the transversal and the linear order. In particular, since the transfer v is a homomorphism from G into the abelian group H/H' , we see that $G' \subseteq \ker(v)$, and thus if $x, y \in G$ and $x \equiv y \pmod{G'}$, it follows that $v(x) = v(y)$, and thus $V(x) \equiv V(y) \pmod{H'}$.

At one point in our proof of Yoshida's theorem, we will need to consider the degenerate case where $H = G$. In that situation, we can take $T = \{1\}$, and we see that the corresponding pretransfer is the identity map. It follows that if $V : G \rightarrow G$ is any pretransfer, then $V(g) \equiv g \pmod{G'}$.

10.6. Lemma. *Let $M \triangleleft P$, where P is a p -group and $|P : M| = p$, and let $V : P \rightarrow M$ be a pretransfer map. Choose a transversal T for M in P . Then for $x \in P$, we have*

$$(a) \text{ If } x \in M, \text{ then } V(x) \equiv \prod_{t \in T} x^t \pmod{M'}.$$

$$(b) \text{ If } x \notin M, \text{ then } V(x) \equiv x^p \pmod{M'}.$$

Proof. First, observe that modulo M' , the pretransfer V is uniquely determined, and so we can compute it using any convenient transversal. Also, since $M \triangleleft P$, it follows that the set $S = \{t^{-1} \mid t \in T\}$ is a transversal for M in P . (One way to see this is to observe that the coset Mt^{-1} is the inverse of Mt in the factor group P/M , which is closed under taking inverses.)

If $x \in M$, we use the transversal S to compute $V(x)$. We have $sxs^{-1} \in M$, and thus $Msx = Ms$, and it follows that $s \cdot x = s$. Then $sx(s \cdot x)^{-1} = sxs^{-1} = x^t$, where $t \in T$ and $s = t^{-1}$. Thus

$$V(x) \equiv \prod_{s \in S} sxs^{-1} \equiv \prod_{t \in T} x^t \pmod{M'},$$

and this proves (a).

Now let $x \in P - M$. Then the set $U = \{x^i \mid 0 \leq i < p\}$ is a transversal for M in P , and this is the transversal we use to compute $V(x)$. To determine $u \cdot x$ for $u \in U$, consider first the case $u = x^i$ for $0 \leq i < p - 1$. Clearly $u \cdot x = x^{i+1}$, and the corresponding factor in the computation of $V(x)$ is $ux(u \cdot x)^{-1} = 1$. The remaining case is $u = x^{p-1}$, where we have $u \cdot x = 1$. The corresponding factor in this case is $ux(u \cdot x)^{-1} = x^p$. Multiplying the factors for $u \in U$, we get $V(x) \equiv x^p \pmod{M'}$, as wanted. ■

Before we state our next result, we recall that if M is a p -group, then the Frattini factor group $M/\Phi(M)$ is elementary abelian, and thus in particular, $M' \subseteq \Phi(M)$. In fact, we can say more: $\Phi(M)/M'$ is exactly the set of p th powers of elements of the abelian group M/M' .

10.7. Lemma. *Let $M \triangleleft P$, where P is a p -group and $|P : M| = p$. Let $V : P \rightarrow M$ be a pretransfer map, and assume that $V(M) \not\subseteq \Phi(M)$. Then $C_p \wr C_p$ is a homomorphic image of P .*

Proof. Write $\bar{P} = P/\Phi(M)$, and observe that since $M' \subseteq \Phi(M)$, the element $\overline{V(x)} \in \bar{P}$ is uniquely determined for all elements $x \in P$. By hypothesis, $V(M) \not\subseteq \Phi(M)$, and thus we can choose an element $x \in M$ such that $V(x) \notin \Phi(M)$. Then $\overline{V(x)} \neq 1$, and by Lemma 10.6(a), we have

$$1 \neq \overline{V(x)} = \prod_{t \in T} \overline{x^t},$$

where T is a transversal for M in P .

Since $(\bar{x})^p = 1$ and $|T| = p$, it follows that the elements $\overline{x^t}$ are not all equal, and thus since \bar{M} is elementary abelian and $|\bar{P} : \bar{M}| = p$, we see that the elements $\overline{x^t}$ are distinct, and they form a full conjugacy class in \bar{P} . The product of the elements in this class is not the identity, and thus Corollary 10.5 guarantees that $C_p \wr C_p$ is a homomorphic image of \bar{P} . It is therefore also a homomorphic image of P , as wanted. ■

Next, we present a general transfer theory result.

10.8. Theorem (Transitivity of transfer). *Let G be a group, and suppose that $H \subseteq K \subseteq G$, where $|G : H| < \infty$. Let*

$$\begin{aligned} U &: G \rightarrow K, \\ W &: K \rightarrow H \text{ and} \\ V &: G \rightarrow H \end{aligned}$$

be pretransfer maps. Then for all $g \in G$, we have $V(g) \equiv W(U(g)) \pmod{H'}$.

Proof. Let T be the right transversal for K in G that was used to construct the pretransfer map U . Thus

$$U(g) = \prod_{t \in T} k_t,$$

where $k_t = tg(t \cdot g)^{-1} \in K$, and the factors k_t are multiplied in some definite but unspecified order. Let $w : K \rightarrow H/H'$ be the transfer, so that $w(k)$ is the coset of H' in H that contains $W(k)$ for $k \in K$. Since w is a homomorphism, we have

$$w(U(g)) = \prod_{t \in T} w(k_t),$$

and thus

$$W(U(g)) \equiv \prod_{t \in T} W(k_t) \pmod{H'}.$$

Now let S be the right transversal for H in K that was used to construct the pretransfer map W . Then

$$W(k_t) = \prod_{s \in S} h_{t,s},$$

where $h_{t,s} = sk_t(s \cdot k_t)^{-1} \in H$, and where for each element $t \in T$, the multiplication is carried out in some definite but unspecified order. Working modulo H' , the order of these factors is irrelevant, and we have

$$W(U(g)) \equiv \prod_{\substack{t \in T \\ s \in S}} h_{t,s} \pmod{H'}.$$

We will show that the set $ST = \{st \mid s \in S, t \in T\}$ is a right transversal for H in G , and that $(st)g((st) \cdot g)^{-1} = h_{t,s}$. It will follow that $V(g)$ is congruent modulo H' to the product (in any particular order) of the elements $h_{t,s}$ for $s \in S$ and $t \in T$, and this will complete the proof.

Let $x \in G$ be an arbitrary element. Then $Kx = Kt$ for some element $t \in T$, and we have $xt^{-1} \in K$. Then $H(xt^{-1}) = Hs$ for some element $s \in S$, and thus $Hx = Hst$. This shows that the coset Hx contains st , and we must show that st is the unique element of ST contained in Hx . Suppose then that $Hst = Hs't'$, where $s' \in S$ and $t' \in T$. Since Hs and Hs' are contained in K , it follows that $Kt = Kt'$, and thus $t = t'$ because T is a right transversal for K in G . Now $Hst = Hs't' = Hs't$, and hence $Hs = Hs'$, and we conclude that $s = s'$ because S is a right transversal for H in K . This shows that ST is indeed a right transversal for H in G , as claimed.

Write $(st) \cdot g = s't'$, where $s' \in S$ and $t' \in T$. Then $Hstg = Hs't'$, and since Hs and Hs' are contained in K , we have $Ktg = Kt'$, and thus $t \cdot g = t'$ and $k_t = tg(t \cdot g)^{-1} = tg(t')^{-1}$. Also,

$$Hsk_t = Hstg(t')^{-1} = Hs't'(t')^{-1} = Hs',$$

and thus $s \cdot k_t = s'$ and $h_{t,s} = sk_t(s \cdot k_t)^{-1} = sk_t(s')^{-1}$. Using the equations

$$k_t = tg(t')^{-1} \quad \text{and} \quad h_{t,s} = sk_t(s')^{-1},$$

we obtain

$$\begin{aligned} (stg)((st) \cdot g)^{-1} &= stg(s't')^{-1} \\ &= stg(t')^{-1}(s')^{-1} \\ &= sk_t(s')^{-1} \\ &= h_{t,s}. \end{aligned}$$

Now multiplication over $t \in T$ and $s \in S$ yields $V(g) \equiv W(U(g)) \pmod{H'}$, as wanted. ■

Finally, we state a fairly technical sufficient condition for a p -group to have a homomorphic image isomorphic to $C_p \wr C_p$. It is this result that we will use in the proof of Yoshida's theorem. Recall that we write $o(x)$ to denote the order of an element x .

10.9. Theorem. *Let $S < P$, where P is a p -group, and let $V : P \rightarrow S$ be a pretransfer. Fix an element $x \in P$, and write $R = \langle s \in S \mid o(s) < o(x) \rangle$. If $V(x) \notin R\Phi(S)$, then $C_p \wr C_p$ is a homomorphic image of P .*

Proof. Since $S < P$, we can choose a maximal subgroup M of P with $S \subseteq M$, and we let $U : P \rightarrow M$ and $W : M \rightarrow S$ be pretransfers. If $U(x) \in \Phi(M)$, then $U(x)$ is a p th power modulo M' , and we can write $U(x) \equiv y^p \pmod{M'}$ for some element $y \in M$. Working mod S' , the pretransfer W yields the transfer homomorphism $w : M \rightarrow S/S'$, and $M' \subseteq \ker(w)$ since w maps to an abelian group. We thus have

$$V(x) \equiv W(U(x)) \equiv W(y^p) \equiv W(y)^p \pmod{S'},$$

where the first congruence holds by Theorem 10.8; the second holds because $U(x) \equiv y^p \pmod{M'}$ and $M' \subseteq \ker(w)$, and the third congruence holds because w is a homomorphism. But $W(y) \in S$, so $W(y)^p \in \Phi(S)$, and thus $V(x) \in \Phi(S)$ since $S' \subseteq \Phi(S)$. This is a contradiction since we assumed that $V(x) \notin R\Phi(S)$, and we conclude that $U(x) \notin \Phi(M)$. If $x \in M$, the result follows by Lemma 10.7.

We can assume now that $x \notin M$, and thus $x \neq 1$ and $o(x^p) < o(x)$. We work to derive a contradiction in this case. Lemma 10.6(b) yields $x^p \equiv U(x) \pmod{M'}$, and thus $V(x) \equiv W(U(x)) \equiv W(x^p) \pmod{S'}$. (Note that we cannot carry this one step farther and write $W(x)^p$ because W is defined only on M , but $x \notin M$.)

By the transfer-evaluation lemma (Lemma 5.5), we know that $W(x^p)$ is congruent modulo S' to a product of conjugates of x^p lying in S . These conjugates are elements of S having smaller order than x , and thus they lie

in $R \subseteq R\Phi(S)$. Since also $S' \subseteq R\Phi(S)$, we conclude that $V(x) \in R\Phi(S)$, contrary to hypothesis. ■

As we mentioned, when Yoshida proved his result, he used character theory, and in particular, he appealed to a representation-theoretic result known as Mackey's theorem. We replace this with the next result, which is a transfer analog of Mackey's theorem. To state the Mackey transfer theorem, we consider the decomposition of a group G into (H, K) -**double cosets**, where H and K are arbitrary subgroups of G . These double cosets are the subsets of G of the form HgK , where $g \in G$. Clearly, HgK is the orbit containing g of the action of the external direct product $H \times K$ on G defined by $g \cdot (h, k) = h^{-1}gk$. Since the sets HgK are orbits in an appropriate action, we see that distinct (H, K) -double cosets are disjoint, and they partition G .

We say that a subset $X \subseteq G$ is a set of **representatives** for the (H, K) -double cosets in G if each of these double cosets contains exactly one element of X . If X is such a set of representatives, then the distinct (H, K) -double cosets in G are exactly the double cosets HxK for $x \in X$, and in particular, $|X|$ is equal to the number of these double cosets.

Note that the double coset HgK is invariant under left multiplication by elements of H , and thus it is a union of right cosets of H . Since G acts by right multiplication on the right cosets of H , the subgroup K acts by right multiplication on these cosets, and it is easy to see that the right cosets of H that comprise the double coset HgK are exactly the members of the K -orbit containing Hg in this action.

Now assume that $|G : H| < \infty$, so that H has just finitely many right cosets in G . Then each double coset HgK is the disjoint union of the finitely many right cosets of H that it contains. These cosets of H form the K -orbit containing Hg , and so we can use the fundamental counting principle to determine their number. The stabilizer of Hg in G is H^g , and it follows that the size of the K -orbit containing Hg is $|K : K \cap H^g|$, and so this is the number of right cosets of H in the double coset HgK . In particular, this number is finite, and so we have $|K : K \cap H^g| < \infty$. Furthermore, since the total number of right cosets of H in G is finite and each (H, K) -double coset is a union of some of these, it follows from the fact that the distinct double cosets are disjoint that there are only finitely many of them, and thus if X is a set of representatives for the (H, K) -double cosets in G , we have $|X| < \infty$.

10.10. Theorem (Mackey transfer). *Let X be a set of representatives for the (H, K) -double cosets in a group G , where H and K are subgroups, and $|G : H| < \infty$. Let $V : G \rightarrow H$ be a pretransfer map, and for each element $x \in X$, let $W_x : K \rightarrow K \cap H^x$ be a pretransfer map. Then for $k \in K$, we*

have

$$V(k) \equiv \prod_{x \in X} xW_x(k)x^{-1} \pmod{H'}.$$

Proof. First, observe that $W_x(k) \in K \cap H^x \subseteq H^x$, and that $W_x(k)$ is uniquely determined modulo $(K \cap H^x)' \subseteq (H^x)' = (H')^x$. It follows that $xW_x(k)x^{-1} \in H$, and this element is uniquely determined modulo H' . Thus the product on the right is an element of H that is uniquely determined modulo H' , and the order in which the factors is multiplied is irrelevant.

For each element $x \in X$, let S_x be the right transversal for $K \cap H^x$ in K used to construct the pretransfer W_x . Then $|S_x| = |K : K \cap H^x|$, which is the number of right cosets of H in HxK . In fact, these right cosets form the K -orbit of Hx under right multiplication. Since $K \cap H^x$ is the stabilizer of Hx in K , it follows that the elements of a right transversal for $K \cap H^x$ in K carry the coset Hx to all of the different members of this K -orbit. This shows that the cosets Hxs for $s \in S_x$ are all of the right cosets of H in HxK . As x runs over X and s runs over S_x , therefore, we account for each right coset of H in G exactly once, and thus the disjoint union

$$T = \bigcup_{x \in X} xS_x$$

is a right transversal for H in G . It follows that

$$V(k) \equiv \prod_{x \in X} \prod_{s \in S_x} xsk((xs) \cdot k)^{-1} \pmod{H'}$$

for all elements $k \in G$. We will complete the proof by showing that if $k \in K$, then for all elements $x \in X$, we have

$$\prod_{s \in S_x} xsk((xs) \cdot k)^{-1} \equiv xW_x(k)x^{-1} \pmod{H'}.$$

We need to compute $(xs) \cdot k$, where $x \in X$, $s \in S_x$ and $k \in K$. This element of T lies in the coset $Hxsk$, which is contained in the double coset HxK because $s \in S_x \subseteq K$ and $k \in K$. It follows that $(xs) \cdot k$ lies in xS_x , and so we can write $(xs) \cdot k = xs'$, where $s' \in S_x$. Then $Hxsk = Hxs'$, and if we left-multiply by x^{-1} , we get $(H^x)sk = (H^x)s'$, and so $sk(s')^{-1} \in H^x$. But also $sk(s')^{-1} \in K$ since $s, s' \in S_x \subseteq K$ and $k \in K$, and thus we have $sk(s')^{-1} \in K \cap H^x$. It follows that

$$(K \cap H^x)sk = (K \cap H^x)s',$$

and thus $s \cdot k = s'$, where here, the dot denotes the action of K on the right transversal S_x for $K \cap H^x$ in K . Then

$$xsk((xs) \cdot k)^{-1} = xsk(xs')^{-1} = xsk(s')^{-1}x^{-1} = x(sk(s \cdot k)^{-1})x^{-1},$$

and this is an equality of elements of H . Now multiply over $s \in S_x$ in some fixed but arbitrary order, and work modulo H' to get

$$\prod_{s \in S_x} xsk((xs) \cdot k)^{-1} \equiv x \left(\prod_{s \in S_x} sk(s \cdot k)^{-1} \right) x^{-1} \equiv xW_x(k)x^{-1} \pmod{H'},$$

as wanted. ■

Yoshida's theorem asserts something about a Sylow p -subgroup P of G under the assumption that $\mathbf{N}_G(P)$ does not control p -transfer. The following lemma will allow us to exploit the failure of transfer control in the proof of Yoshida's theorem.

10.11. Lemma. *Let $P \subseteq N \subseteq G$, where P is a Sylow p -subgroup of the finite group G and N is a subgroup that does not control p -transfer in G . Then there exists a subgroup $M \triangleleft N$, with $|N : M| = p$, and such that $U(G) \subseteq M$ for all pretransfer maps $U : G \rightarrow N$.*

Proof. Let $V : G \rightarrow P$ and $W : N \rightarrow P$ be pretransfer maps, and let v and w be the corresponding transfer homomorphisms obtained by composing V and W with the canonical homomorphism $P \rightarrow P/P'$. If $U : G \rightarrow N$ is a pretransfer, it follows by transitivity of transfer (Theorem 10.8) that $v(G) = w(U(G)) \subseteq w(N)$. Now $G/\mathbf{A}^p(G) \cong v(G)$ and $N/\mathbf{A}^p(N) \cong w(N)$, and since we are assuming that $G/\mathbf{A}^p(G)$ and $N/\mathbf{A}^p(N)$ are not isomorphic, it follows that $v(G) \neq w(N)$, and thus $v(G) < w(N)$.

Since $w(N)$ is a p -group and $v(G)$ is a proper subgroup, there exists a subgroup L such that $v(G) \subseteq L \triangleleft w(N)$ and $|w(N) : L| = p$. By the correspondence theorem applied to the homomorphism $w : N \rightarrow P/P'$, the inverse image of L in N is a subgroup M of N such that $M \triangleleft N$, and $|N : M| = |w(N) : L| = p$. Also, since $w(U(G)) = v(G) \subseteq L$ for an arbitrary pretransfer map $U : G \rightarrow N$, it follows that $U(G) \subseteq M$, as wanted. ■

Finally, we are ready to prove Yoshida's theorem.

Proof of Theorem 10.1. Assume that $N = \mathbf{N}_G(P)$ does not control p -transfer in G , and let $V : G \rightarrow N$ be a pretransfer map. By Lemma 10.11, we can choose a subgroup $M \triangleleft N$ with $|N : M| = p$, and such that $V(G) \subseteq M$, and we note that $N' \subseteq M$.

Choose an element $n \in N - M$ such that the order $o(n)$ is as small as possible. If q is any prime divisor of $o(n)$, then $o(n^q) < o(n)$, and so $n^q \in M$, and thus the image of n in N/M has order q . But $|N/M| = p$, and it follows that $q = p$, and thus $o(n)$ is power of p . Since P is the unique Sylow p -subgroup of N , we have $n \in P$.

Now let X be a set of representatives for the (N, P) -double cosets in G , and for each element $x \in X$, fix a pretransfer map $W_x : P \rightarrow P \cap N^x$.

Since $n \in P$, we can apply the Mackey transfer theorem (Theorem 10.10) to deduce that

$$V(n) \equiv \prod_{x \in X} xW_x(n)x^{-1} \pmod{N'}.$$

Also, $V(n) \in V(G) \subseteq M$, and since also $N' \subseteq M$, it follows that

$$\prod_{x \in X} xW_x(n)x^{-1} \in M.$$

Since $P \subseteq N$, one of the (N, P) -double cosets is $NIP = N$, and so exactly one member of X lies in N . If we call this element y , we see that $P \cap N^y = P$ and thus W_y is a pretransfer from P to itself, and we have $W_y(n) \equiv n \pmod{P'}$. Since $P' \subseteq N' \subseteq M$ and $n \notin M$, it follows that $W_y(n) \notin M = M^y$, and thus $yW_y(n)y^{-1} \notin M$.

The product of the elements $xW_x(n)x^{-1}$ lies in M , and since the factor corresponding to $x = y$ does not lie in M , it follows that some other factor must also fail to lie in M . There exists an element $x \in G - N$, therefore, and a pretransfer map $W : P \rightarrow P \cap N^x$, such that $xW(n)x^{-1} \notin M$. We thus have $W(n) \in (P \cap N^x) - (P \cap M^x)$.

Now writing $S = P \cap N^x$ and $Q = P \cap M^x$, we have $Q \subseteq S \subseteq P$ and $W(n) \in S - Q$. By the choice of the element n , we know that all elements of N with order smaller than $o(n)$ lie in M , and thus all elements of N^x with order smaller than $o(n)$ lie in M^x . It follows that the subgroup $R = \langle s \in S \mid o(s) < o(n) \rangle$ is contained in Q . Also,

$$|S : Q| = |S : S \cap M^x| = |SM^x : M^x| \leq |N^x : M^x| = p,$$

and therefore, $\Phi(S) \subseteq Q$. Thus $R\Phi(S) \subseteq Q$, and since $W(n) \notin Q$, we have $W(n) \notin R\Phi(S)$.

Finally, recall that $x \notin N = N_G(P)$, and thus $P^x \neq P$. But P^x is the unique Sylow p -subgroup of G contained in N^x , and thus $P \not\subseteq N^x$, and we have $S = P \cap N^x < P$. By Theorem 10.9, therefore, $C_p \wr C_p$ is a homomorphic image of P . ■

Problems 10A

10A.1. Show that a 2-group P is regular if and only if it is abelian.

Hint. First, observe that factor groups of regular p -groups are regular. If P is a minimal counterexample to the problem, show that $|P'| = 2$.

10A.2. Let P be a regular p -group. Show that the set $\{x \in P \mid x^p = 1\}$ is a subgroup.

Hint. First, observe that subgroups of regular p -groups are regular. Suppose that P is a minimal counterexample to the problem. Show that if $x, y \in P$, where x has order p , then some proper subgroup of P contains both x and x^y , and deduce that $[x, y]^p = 1$. Conclude that the p th power of every element of P' is trivial.

10A.3. Let P be a p -group with $|\mathbf{Z}(P)| = p$, and let A be abelian and have index p in P . If $\mathbf{Z}(P)$ is a direct factor of A , deduce that P is isomorphic to a subgroup of $C_p \wr C_p$, and show that A is elementary abelian.

10A.4. Suppose that $P \in \text{Syl}_2(G)$, and that P is isomorphic to the direct product of the quaternion group Q_8 with the cyclic group C_2 . Show that $G' < G$.

Hint. Observe that $C_2 \wr C_2 \cong D_8$. Also, if $N = \mathbf{N}_G(P)$, show that N/P has a nontrivial fixed point in its natural action on $P/\Phi(P)$.

10A.5. Let $Q \subseteq P$, where P is a p -group and $|P : Q| = p^2$, and suppose that $Q \cap \mathbf{Z}(P) = 1$. Show that P is isomorphic to a subgroup of $C_p \wr C_p$.

10A.6. Let G act transitively on a set Ω , and let H be a point stabilizer. Show that G is 2-transitive on Ω if and only if $G = H \cup HgH$ for some element $g \in G$.

10A.7. Let $A \triangleleft P$, where $|P : A| = p$ and A is an elementary abelian p -group. Suppose that $P - A$ contains an element of order p and also an element of order p^2 . Show that $C_p \wr C_p$ is a homomorphic image of P .

10B

A group is **metacyclic** if it has a cyclic normal subgroup with a cyclic factor group. In this section, we use Yoshida's theorem to prove the following result of B. Huppert.

10.12. Theorem (Huppert). *Let $P \in \text{Syl}_p(G)$, where G is a finite group and $p > 2$, and suppose that P is nonabelian and metacyclic. Then p divides $|G : G'|$.*

We begin with some easy observations.

10.13. Lemma. *Let P be a metacyclic group.*

- (a) *If $U \triangleleft P$, then P/U is metacyclic.*
- (b) *If $V \subseteq P$, then V is metacyclic.*

Proof. Let $C \triangleleft P$, where C and P/C are cyclic. For (a), write $\bar{P} = P/U$. Then $\bar{C} \triangleleft \bar{P}$, and \bar{C} is a homomorphic image of C , and thus \bar{C} is cyclic. Also, $\bar{P}/\bar{C} \cong P/UC$, and this is a homomorphic image of the cyclic group P/C . Thus \bar{P}/\bar{C} is cyclic, and hence \bar{P} is metacyclic, as required. For (b), observe that $V \cap C \triangleleft V$ and $V \cap C$ is cyclic since it is a subgroup of C . Also, $V/(V \cap C) \cong VC/C$, which is a subgroup of P/C , and so it is cyclic. It follows that V is metacyclic. ■

10.14. Lemma. *Assume that $p > 2$. Then the group $W = C_p \wr C_p$ is not a homomorphic image of a metacyclic group.*

Proof. By Lemma 10.13(a), it suffices to show that W is not metacyclic. If W is metacyclic, however, then W' is contained in a cyclic normal subgroup, and so W' is cyclic. This is not the case, however, since W' is elementary abelian of order $p^{p-1} > p$ by Lemma 10.3(b). ■

Now assume the hypotheses of Theorem 10.12. As we have just seen, $C_p \wr C_p$ cannot be a homomorphic image of the metacyclic Sylow p -subgroup P , and hence Theorem 10.1 guarantees that $N = \mathbf{N}_G(P)$ controls p -transfer in G . If we can show that $\mathbf{A}^p(N) < N$, therefore, it will follow that $\mathbf{A}^p(G) < G$, and thus p divides $|G : G'|$, as wanted. It suffices, therefore, to prove the following result.

10.15. Theorem. *Let $P \triangleleft N$, where N is a finite group and $P \in \text{Syl}_p(N)$, and assume that P is nonabelian and metacyclic, and that $p > 2$. Then p divides $|N : N'|$.*

We need Maschke's theorem, which is usually viewed as belonging to representation theory, but which is useful when considering coprime actions on elementary abelian p -groups. We use the more-or-less standard proof of Maschke's theorem to establish Theorem 10.16, whose statement is somewhat more general than the usual statement of Maschke's theorem.

10.16. Theorem (Maschke). *Let K be a group of finite order m , and suppose that K acts via automorphisms on a group V with subgroups U and W such that $V = U \times W$, where U is abelian and K -invariant. Assume that the map $u \mapsto u^m$ is both injective and surjective on U . Then there exists a K -invariant subgroup $N \triangleleft V$ such that $V = U \times N$.*

Observe that if U is finite and has order coprime to m , then the map $u \mapsto u^m$ is automatically both injective and surjective. This is because it has an inverse, namely the map $u \mapsto u^n$, where the integer n is chosen so that $mn \equiv 1 \pmod{|U|}$.

In the standard version of Maschke's theorem, V is a vector space over some field F , and U is a given K -invariant subspace. In that case, it is

automatic that U is a direct summand of V , and so no explicit mention of W appears in the usual statement of the result. Here, of course, the group V is written additively, and so the key requirement is that the map $u \mapsto m \cdot u$ should be injective and surjective, and this happens if the characteristic of the field F does not divide m . (And it fails otherwise.)

We need the following case of Maschke's theorem for the proof of Theorem 10.15.

10.17. Corollary. *Let K be a finite group that acts via automorphisms on an elementary abelian p -group V , and assume that p does not divide $|K|$. Suppose that $U \subseteq V$ is a K -invariant subgroup. Then there exists a K -invariant subgroup $N \subseteq V$ such that $V = U \times N$.*

Proof. Write $m = |K|$ and observe that $|U|$ is coprime to m , so that as we observed, the map $u \mapsto u^m$ is both injective and surjective on U , as required for Theorem 10.16. It suffices, therefore, to show that $V = U \times W$ for some subgroup $W \subseteq V$. As we mentioned in the discussion preceding Theorem 10.4, this follows easily by viewing V as a vector space over the field $\mathbb{Z}/p\mathbb{Z}$. ■

Proof of Theorem 10.16. Since $V = U \times W$, we can define the map $\theta : V \rightarrow U$ by setting $\theta(uw) = u$ for $u \in U$ and $w \in W$, and we observe that θ is a homomorphism and that $\theta(u) = u$ for $u \in U$. Now let $x \in V$ and $k \in K$. Then $\theta(x^k) \in U$, and since U is K -invariant, we see that $\theta(x^k)^{k^{-1}} \in U$. Since K is finite, we can define the map $\varphi : V \rightarrow U$ by

$$\varphi(x) = \prod_{k \in K} \theta(x^k)^{k^{-1}},$$

and we observe that this is well defined since each factor in the product lies in U and U is abelian. In fact, φ is a homomorphism since if $x, y \in V$ and $k \in K$, we have $(xy)^k = x^k y^k$, and hence

$$\begin{aligned} \varphi(xy) &= \prod_{k \in K} \theta((xy)^k)^{k^{-1}} \\ &= \prod_{k \in K} (\theta(x^k) \theta(y^k))^{k^{-1}} \\ &= \prod_{k \in K} \theta(x^k)^{k^{-1}} \prod_{k \in K} \theta(y^k)^{k^{-1}} \\ &= \varphi(x) \varphi(y), \end{aligned}$$

where, of course, the third equality holds because U is abelian.

Now let $N = \ker(\varphi)$. To show that N is K -invariant, let $a \in K$ and compute that

$$\varphi(x^a)^{a^{-1}} = \left(\prod_{k \in K} \theta(x^{ak})^{k^{-1}} \right)^{a^{-1}} = \prod_{k \in K} \theta(x^{ak})^{(ak)^{-1}} = \varphi(x),$$

where the last equality holds because ak runs over all elements of K as k does. It follows that $\varphi(x^a) = \varphi(x)^a$, and hence if $\varphi(x) = 1$, then also $\varphi(x^a) = 1$ for all $a \in K$. This shows that N is K -invariant, as claimed.

Of course, $N = \ker(\varphi) \triangleleft V$, so to complete the proof, we must show that $U \cap N = 1$ and $UN = V$. If $u \in U$, then $u^k \in U$ for all $k \in K$, and thus $\theta(u^k)^{k^{-1}} = (u^k)^{k^{-1}} = u$, and it follows that $\varphi(u) = u^m$, where we recall that $m = |K|$. By hypothesis, therefore, the restriction of φ to U is both injective and surjective, and in particular, $U \cap N = U \cap \ker(\varphi) = 1$. Finally, we have $\varphi(UN) = \varphi(U) = U$, and thus also $\varphi(V) = U$. Since $UN \supseteq N$, it follows by the correspondence theorem that $UN = V$, as required. ■

We can now prove Theorem 10.15, and as we have observed, Huppert's theorem (Theorem 10.12) will then follow.

Proof of Theorem 10.15. Recall that $P \triangleleft N$, where P is a nonabelian metacyclic Sylow p -subgroup of N , and $p > 2$. Our goal is to show that N has an abelian homomorphic image of order divisible by p , and we proceed by induction on $|P|$.

Since P is metacyclic, P' is cyclic, and of course $P' \triangleleft N$. Also $P' > 1$, and thus P' has a unique subgroup of order p , which is necessarily normal in N . Now let Y be an arbitrary normal subgroup of order p in N . Then P/Y is a normal Sylow p -subgroup of N/Y , and it is metacyclic by Lemma 10.13(a). If P/Y is nonabelian, it follows by the inductive hypothesis that N/Y has an abelian homomorphic image of order divisible by p , and thus N has such a homomorphic image and we are done. We can assume, therefore, that P/Y is abelian, and thus $P' \subseteq Y$. It follows that $Y = P'$, and thus $|P'| = p$, and P' is the unique normal subgroup of order p in N .

Since $|P'| = p$, it follows that P' is central in P , and thus P has nilpotence class 2. Because $p > 2$, Theorem 4.8(a) guarantees that the set $V = \{x \in P \mid x^p = 1\}$ is a subgroup of P , and of course, $V \triangleleft N$. Also V is metacyclic by Lemma 10.13(b), and since every cyclic subgroup and cyclic factor group of V has order at most p , it follows that $|V| \leq p^2$. Furthermore, since P is not cyclic and $p > 2$, it follows by Theorem 6.11 that P has more than one subgroup of order p , and we deduce that $|V| = p^2$, and V is an elementary abelian p -group.

Now write $Z = \mathbf{Z}(P)$. If $V \subseteq Z$, then P is in the kernel of the conjugation action of N on V , and so N/P acts on V . This is a coprime action, and

since P' is an invariant subgroup of order p , it follows by Maschke's theorem (or more precisely, by Corollary 10.17) that we can write $V = P' \times W$, where W is (N/P) -invariant, and thus $W \triangleleft N$. But $|W| = p$, and this is a contradiction since P' is the unique normal subgroup of order p in N . We conclude that $V \not\subseteq Z$.

Since $P' \subseteq Z$, the group P/Z is abelian. Also, it follows that for each element $x \in P$, the map $[\cdot, x]$ is a homomorphism. If $y \in P$, therefore, we have $[y^p, x] = [y, x]^p = 1$, where the second equality holds because $|P'| = p$. Thus x centralizes y^p , and since $x \in P$ is arbitrary, we see that $y^p \in Z$ for all $y \in P$, and we conclude that P/Z is elementary abelian.

Now N acts on P/Z , and P is contained in the kernel of this action because P/Z is abelian. It follows that N/P acts on P/Z , and of course, this is a coprime action. Also VZ/Z is an invariant subgroup, and hence by Maschke's theorem, we can write $P/Z = (VZ/Z) \times (H/Z)$, where H/Z is (N/P) -invariant, and thus $H \triangleleft N$. Also $V \cap H \subseteq VZ \cap H = Z$, and since $V \not\subseteq Z$, it follows that $V \not\subseteq H$, and thus $|V \cap H| < p^2$. We conclude that H has a unique subgroup of order p , and thus H is cyclic.

Now V is abelian and Z is central, and thus VZ is abelian. Then $VZ \neq P$, so $VZ/Z < P/Z$, and thus H/Z is nontrivial, and H is not central in P . Now write $C = \mathbf{C}_N(H)$, so that $P \not\subseteq C$, and thus N/C has order divisible by p . Also, N/C is isomorphically embedded in $\text{Aut}(H)$, and since H is cyclic, $\text{Aut}(H)$ is abelian, and thus N/C is an abelian homomorphic image of N with order divisible by p . It follows that p divides $|N : N'|$, as required. ■

Problems 10B

10B.1. Given a prime p and an integer $n > 0$, let $C = \langle x \rangle$ be a cyclic group of order p^n . Let $\sigma \in \text{Aut}(G)$ with $x^\sigma = x^{p+1}$, and let $P = C \rtimes \langle \sigma \rangle$. Show that P is a metacyclic p -group with nilpotence class n .

Hint. Use Theorem 4.7.

Note. This problem shows that metacyclic p -groups can have arbitrarily large nilpotence class, and we know that if $p > 2$, such a group cannot have $C_p \wr C_p$ as a homomorphic image. It follows that Yoshida's theorem is strictly stronger than the assertion that a Sylow normalizer controls p -transfer if the Sylow p -subgroup has nilpotence class less than p .

10B.2. Let $E \triangleleft G$, where E is an elementary abelian p -group, and suppose that $|G : C_G(E)|$ is not divisible by p . Show that $E \subseteq \text{Soc}(G)$.

10C

If H is an arbitrary subgroup of a finite group G , then of course, the derived subgroup G' is contained in the kernel of the transfer homomorphism $G \rightarrow H/H'$. In this section we discuss another connection between G' and transfer; we consider what happens if G' plays the role of H .

10.18. Theorem. *Let G be a finite group. Then the transfer homomorphism $G \rightarrow G'/G''$ is the trivial map.*

For applications within group theory, we generally seek results (such as Yoshida's theorem) that allow us to prove in certain cases that the transfer homomorphism is nontrivial. But Theorem 10.18, does just the opposite: it shows that the transfer map is trivial when the target is the derived subgroup. There do not seem to be many group-theoretic applications of this result, but it does have applications to algebraic number theory, and in particular to class field theory. (In that context, Theorem 10.18, which was first proved by P. Furtwängler, is usually called the “principal ideal theorem”.) We have decided to present this result because it is striking and easy to state, and yet it seems quite difficult to prove. The proof we are about to present is essentially due to G. Hochschild. It uses some elementary ring theory, and so it is quite different in flavor from everything else in this book, but we hope that readers will find it to be accessible.

Let G be a finite group and let R be any ring. (Recall that by definition, rings contain unity elements.) The **group ring** $R[G]$ is the set of formal sums of the form $\sum r_g g$, where the sum runs over $g \in G$, and the coefficients r_g lie in R . Elements of the group ring are added in the obvious way:

$$\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g,$$

and this makes $R[G]$ into an additive group. We view G as a subset of $R[G]$ by identifying the group element $g \in G$ with the sum $\sum r_x x$, where $r_g = 1$ and $r_x = 0$ for $x \neq g$. From this point of view, an arbitrary element $\sum r_g g$ in $R[G]$ is no longer just a formal sum; it is an actual linear combination of the elements of G with coefficients in R .

To define multiplication in $R[G]$, we use the multiplication in G together with the multiplication in R and the distributive law. Thus

$$\left(\sum_{x \in G} r_x x \right) \left(\sum_{y \in G} s_y y \right) = \sum_{g \in G} t_g g,$$

where

$$t_g = \sum_{\substack{x, y \in G \\ xy = g}} r_x s_y.$$

It is routine to check that these definitions of addition and multiplication make $R[G]$ into a ring in which the identity element of G is the unity element.

We mention that the group ring $R[G]$ can be defined even if G is an infinite group, but in that case, the elements of $R[G]$ are just those formal sums $\sum r_g g$ in which all but finitely many of the coefficients r_g are zero. Some of our results hold in this more general setting, and in fact, some of our proofs go through essentially unchanged. Nevertheless, we will generally assume that G is finite in what follows.

We shall need only the integer group ring $\mathbb{Z}[G]$, where \mathbb{Z} is the ordinary ring of integers. In this case, where $R = \mathbb{Z}$, there is a natural connection between the group ring and actions of G on abelian groups, and we will exploit this in the proof of Theorem 10.18.

Suppose that M is an arbitrary additively written abelian group, and let G be a finite group that acts via automorphisms on M . If $x \in M$ and $g \in G$, we would usually write x^g to denote the element of M resulting from the action of g on x , but in this setting, where M is written additively, it is more convenient to write xg in place of x^g . In this notation, we have $x1 = x$ and $(xg)h = x(gh)$ for $x \in M$ and $g, h \in G$. Also, since the given action is assumed to be via automorphisms, we have $(x + y)g = xg + yg$ for $x, y \in M$ and $g \in G$. If $n \in \mathbb{Z}$ and $x \in M$, then of course, xn is just the element that would be written x^n in the standard multiplicative notation, and since the action is via automorphisms, we have $(xn)g = (xg)n$ for $g \in G$, $n \in \mathbb{Z}$ and $x \in M$.

Now let $\sum e_g g \in \mathbb{Z}[G]$, where, of course, $e_g \in \mathbb{Z}$ for $g \in G$. If $x \in M$, we can define a “right action” of the ring $\mathbb{Z}[G]$ on M by setting

$$x \left(\sum e_g g \right) = \sum (xg) e_g.$$

It is routine to check for $\alpha, \beta \in \mathbb{Z}[G]$ and $x, y \in M$ that

- (a) $x(\alpha + \beta) = x\alpha + x\beta$,
- (b) $(x\alpha)\beta = x(\alpha\beta)$,
- (c) $(x + y)\alpha = x\alpha + y\alpha$ and, of course
- (d) $x1 = x$, where 1 is the unity of $\mathbb{Z}[G]$.

In other words, M is a right $\mathbb{Z}[G]$ -module. Of course, if we had started with a “left action” via automorphisms of G on M , so that $g(hx) = (gh)x$ for $g, h \in G$ and $x \in M$, the analogous construction would make M into a left $\mathbb{Z}[G]$, module.

Temporarily putting modules aside, we define the **augmentation** map $\delta : \mathbb{Z}[G] \rightarrow \mathbb{Z}$ by setting

$$\delta \left(\sum e_g g \right) = \sum e_g,$$

so that $\delta(\alpha)$ is simply the sum of the coefficients appearing in $\alpha \in \mathbb{Z}[G]$. It is routine to check that δ is a ring homomorphism, and so its kernel, denoted $\Delta(G)$, is an ideal of $\mathbb{Z}[G]$; it is called the **augmentation ideal**.

10.19. Lemma. *Let G be a finite group. Then $\Delta(G)$ is the additive subgroup of $\mathbb{Z}[G]$ generated by the elements $g - 1$ for $1 \neq g \in G$, and in fact, these generators form a \mathbb{Z} -basis for $\Delta(G)$.*

We should explain what we mean by a “ \mathbb{Z} -basis”. Let M be an additively written finitely generated abelian group, and let $\{x_1, x_2, \dots, x_n\}$ be a generating set. Then the subset of M consisting of elements of the form $\sum e_i x_i$ for $e_i \in \mathbb{Z}$ is clearly a subgroup of M that contains all of the generators x_i . It is thus all of M , and hence every element of M is a linear combination of the form $\sum e_i x_i$. The given generating set is a \mathbb{Z} -basis for M if the only way to get $\sum e_i x_i = 0$ is for all coefficients $e_i = 0$. In this case, each element of M is *uniquely* of the form $\sum e_i x_i$. For example, if G is a finite group, then G is a \mathbb{Z} -basis for the additive group of $\mathbb{Z}[G]$.

Of course, not every finitely generated abelian group has a \mathbb{Z} -basis; those that do are said to be **free abelian** groups. A nontrivial *finite* abelian group, for example, cannot have a \mathbb{Z} -basis, and so it is definitely not free abelian.

In fact, one can define infinite \mathbb{Z} -bases analogously, and the conclusion of Lemma 10.19 holds for infinite groups too.

Proof of Lemma 10.19. Certainly, $\delta(g - 1) = 0$ for $g \in G$, where δ is the augmentation map, and thus $g - 1 \in \ker(\delta) = \Delta(G)$. Now let α be an arbitrary element of $\Delta(G)$, and write $\alpha = \sum e_g g$, with $e_g \in \mathbb{Z}$. Then

$$\alpha = \sum_{1 \neq g \in G} e_g (g - 1) + \left(\sum_{g \in G} e_g \right) 1,$$

and since $\sum e_g = \delta(\alpha) = 0$, we see that α is a \mathbb{Z} -linear combination of the elements $g - 1$ for $1 \neq g \in G$, and hence these elements form a generating set for $\Delta(G)$.

To check that these generators form a \mathbb{Z} -basis, suppose that there exist coefficients $f_g \in \mathbb{Z}$ for $1 \neq g \in G$ such that $\sum f_g (g - 1) = 0$. Then

$$0 = \sum_{1 \neq g \in G} f_g g - \left(\sum_{1 \neq g \in G} f_g \right) 1$$

and since G is a \mathbb{Z} -basis for $\mathbb{Z}[G]$, it follows that the coefficient f_g of g is zero for all nonidentity elements $g \in G$. ■

Suppose that $\{x_1, x_2, \dots, x_n\}$ is a \mathbb{Z} -basis for some additively written abelian group M , and let A be an arbitrary (multiplicative) abelian group.

Choose arbitrary elements $a_i \in A$ for $1 \leq i \leq n$, and define the map $\theta : M \rightarrow A$ by setting

$$\theta\left(\sum e_i x_i\right) = \prod (a_i)^{e_i}.$$

Note that θ is well defined since every element of M is uniquely of the form $\sum e_i x_i$ with $e_i \in \mathbb{Z}$, and it is trivial to check that θ is a group homomorphism. This shows that if M is a free abelian group and A is any abelian group, then there is homomorphism $\theta : M \rightarrow A$ such that θ carries the members of a \mathbb{Z} -basis for M to arbitrarily selected elements of A .

Now let M be a left R -module, and let $X \subseteq R$ and $Y \subseteq M$ be additive subgroups. (The following remarks also apply in the important case where $M = R$, and where X and Y are additive subgroups of R .) Recall that by definition, XY is the set of all (finite) sums and differences of elements of the form xy in M , where $x \in X$ and $y \in Y$. (Equivalently, XY is the additive subgroup of M generated by all products of the form xy .) Observe that if X and Y are finitely generated (as additive groups) by subsets $\{x_i\}$ and $\{y_j\}$ respectively, then XY is finitely generated by the products $x_i y_j$.

In particular, in $\mathbb{Z}[G]$, the augmentation ideal $\Delta(G)$ is an additive subgroup generated by the elements $g - 1$ for $g \in G$, and thus $\Delta(G)^2$ is the additive subgroup generated by elements of the form $(g - 1)(h - 1)$ for $g, h \in G$. Note that $\Delta(G)\mathbb{Z}[G] \subseteq \Delta(G)$ since $\Delta(G)$ is an ideal, and thus $\Delta(G)^2 \subseteq \Delta(G)$.

10.20. Theorem. *Let G be a finite group. Then G/G' is isomorphic to the additive group $\Delta(G)/\Delta(G)^2$ via an isomorphism carrying the coset $G'g$ to the coset $(g - 1) + \Delta(G)^2$.*

Proof. Define $\varphi : G \rightarrow \Delta(G)/\Delta(G)^2$ by setting $\varphi(g) = (g - 1) + \Delta(G)^2$. For elements $x, y \in G$, we have $xy - 1 = (x - 1) + (y - 1) + (x - 1)(y - 1)$, and since $(x - 1)(y - 1) \in \Delta(G)^2$, it follows that $\varphi(xy) = \varphi(x) + \varphi(y)$, and hence φ is a homomorphism. Also, since the additive group $\Delta(G)$ is generated by elements of the form $x - 1$ with $x \in G$, we see that $\Delta(G)/\Delta(G)^2$ is generated by the cosets $(x - 1) + \Delta(G)^2$, and thus $\varphi(G)$ is a generating set for $\Delta(G)/\Delta(G)^2$. But $\varphi(G)$ is a subgroup, and thus it must be the whole group $\Delta(G)/\Delta(G)^2$, and hence φ is surjective. Also, since φ is a homomorphism from G to an abelian group, it follows that $G' \subseteq \ker(\varphi)$. To complete the proof, we show that in fact, $G' = \ker(\varphi)$, and thus φ defines an isomorphism from G/G' onto $\Delta(G)/\Delta(G)^2$.

Next, we construct a map in the opposite direction. By Lemma 10.19, the set $\{g - 1 \mid 1 \neq g \in G\}$ is a \mathbb{Z} -basis for $\Delta(G)$, and since G/G' is an abelian group, there is a homomorphism $\theta : \Delta(G) \rightarrow G/G'$ such that $\theta(g - 1) = G'g$ for $1 \neq g \in G$. (Of course, this formula also holds when $g = 1$ since θ is a homomorphism, and thus $\theta(0)$ is the identity element of G/G' .)

Since θ is a homomorphism from the additive group $\Delta(G)$ to G/G' , and $\theta(g - 1) = G'g$ for all elements $g \in G$, we can apply θ to both sides of the identity $xy - 1 = (x - 1) + (y - 1) + (x - 1)(y - 1)$ to get $G'(xy) = (G'x)(G'y)\theta((x - 1)(y - 1))$ for elements $x, y \in G$. But $G'(xy) = (G'x)(G'y)$, and it follows that $\theta((x - 1)(y - 1))$ is the identity, and thus $(x - 1)(y - 1) \in \ker(\theta)$. The elements $(x - 1)(y - 1)$ generate $\Delta(G)^2$ as an abelian group, however, and thus $\Delta(G)^2 \subseteq \ker(\theta)$.

We have seen that $\ker(\varphi) \supseteq G'$ and that it suffices to prove equality here. To establish the reverse containment, let $k \in \ker(\varphi)$. Since $\varphi(k)$ is the 0 element of $\Delta(G)/\Delta(G)^2$, and by definition, $\varphi(k) = (k - 1) + \Delta(G)^2$, it follows that $k - 1 \in \Delta(G)^2 \subseteq \ker(\theta)$, and thus $G'k = \theta(k - 1)$ is the identity of G/G' , and hence $k \in G'$, as required. ■

Let $K \subseteq G$ be a subgroup, and view $\mathbb{Z}[K] \subseteq \mathbb{Z}[G]$. Let T be a right transversal for K in G , so that each element $g \in G$ is uniquely of the form kt , where $k \in K$ and $t \in T$. If $\alpha \in \mathbb{Z}[G]$ is arbitrary, therefore, we can write

$$\alpha = \sum_{t \in T} \left(\sum_{k \in K} e_{kt} k \right) t = \sum_{t \in T} \alpha_t t,$$

where $e_{kt} \in \mathbb{Z}$ and $\alpha_t = \sum_k e_{kt} k \in \mathbb{Z}[K]$. We refer to α_t as the t -**component** of α with respect to T , and we observe that for each element $t \in T$, the map $f_t : \alpha \mapsto \alpha_t$ from $\mathbb{Z}[G]$ to $\mathbb{Z}[K]$ is a well defined homomorphism of additive groups. We shall need the following technical result.

10.21. Lemma. *Let $K \subseteq G$, where G is a finite group, and let T be a right transversal for K in G such that $1 \in T$. Working in $\mathbb{Z}[G]$, let $\alpha \in \Delta(K)\Delta(G)$, and for $t \in T$, write α_t to denote the t -component of α with respect to T . Then $\alpha_t \in \Delta(K)$ and $\sum_t \alpha_t \in \Delta(K)^2$.*

Proof. Let f_t be the map carrying an element of $\mathbb{Z}[G]$ to its t -component with respect to T , and write $f = \sum_t f_t$. Then f and all of the maps f_t are additive homomorphisms, and our goal is to show that $f_t(\Delta(K)\Delta(G)) \subseteq \Delta(K)$ for all $t \in T$, and that $f(\Delta(K)\Delta(G)) \subseteq \Delta(K)^2$. Since the elements $(k - 1)(g - 1)$ for $k \in K$ and $g \in G$ generate the additive group $\Delta(K)\Delta(G)$, it suffices to prove the lemma in the case $\alpha = (k - 1)(g - 1)$.

First, suppose that $g \in K$. Then $\alpha = (k - 1)(g - 1) \in \mathbb{Z}[K]$, and thus the 1-component of α is α , and all other components are zero. Since $\alpha \in \Delta(K)^2 \subseteq \Delta(K)$ in this case, there is nothing further to prove.

We can now assume that $g \notin K$, and we write $g = hs$, where $h \in K$ and $s \in T - \{1\}$. Then

$$\alpha = (k - 1)(g - 1) = (k - 1)g - (k - 1) = (k - 1)hs - (k - 1)1,$$

and thus $\alpha_s = (k-1)h \in \Delta(K)$ and $\alpha_1 = -(k-1) \in \Delta(K)$. All other components of α are zero, and thus all components lie in $\Delta(K)$, as required. Also, $f(\alpha) = (k-1)h - (k-1) = (k-1)(h-1) \in \Delta(K)^2$, and the proof is complete. ■

10.22. Corollary. *Let $K \subseteq G$, where G is a finite group. Then in $\mathbb{Z}[G]$, we have $\Delta(K)^2 = \Delta(K)\Delta(G) \cap \Delta(K) = \Delta(K)\Delta(G) \cap \mathbb{Z}[K]$.*

Proof. It is clear that $\Delta(K)^2 \subseteq \Delta(K)\Delta(G) \cap \Delta(K) \subseteq \Delta(K)\Delta(G) \cap \mathbb{Z}[K]$, so it is sufficient to show that $\Delta(K)\Delta(G) \cap \mathbb{Z}[K] \subseteq \Delta(K)^2$. Let T be as in Lemma 10.21, and observe that if $\alpha \in \Delta(K)\Delta(G) \cap \mathbb{Z}[K]$ then the 1-component of α is α itself, and all other components are zero. Thus α is the sum of its components, and so $\alpha \in \Delta(K)^2$ by Lemma 10.21. ■

If $K \subseteq G$, then since $\Delta(G)$ is an ideal of $\mathbb{Z}[G]$, we have $\Delta(K)\Delta(G) \subseteq \Delta(G)$. Of course $\Delta(K)\Delta(G)$ is a normal subgroup of the additive group $\Delta(G)$, and in the next several results, we study the factor group $\overline{\Delta(G)} = \Delta(G)/\Delta(K)\Delta(G)$. We use the standard “bar convention”, so that if A is any additive subgroup of $\Delta(G)$, then \overline{A} is the image of A under the canonical homomorphism $\Delta(G) \rightarrow \overline{\Delta(G)}$. In particular, since $\Delta(K) \subseteq \Delta(G)$, we see that $\overline{\Delta(K)}$ is a subgroup of $\overline{\Delta(G)}$.

10.23. Corollary. *Let $K \subseteq G$, where G is a finite group. Working in $\mathbb{Z}[G]$, let*

$$\overline{\Delta(G)} = \frac{\Delta(G)}{\Delta(K)\Delta(G)}.$$

Then $\overline{\Delta(K)} \cong K/K'$, where $\overline{k-1}$ maps to $K'k$ for elements $k \in K$.

Proof. The map $k-1 \mapsto \overline{k-1}$ defines a homomorphism from $\Delta(K)$ onto $\overline{\Delta(K)}$ with kernel equal to $\Delta(K) \cap \Delta(G)\Delta(K)$. By Corollary 10.22, this kernel is equal to $\Delta(K)^2$, and thus $\overline{\Delta(K)} \cong \Delta(K)/\Delta(K)^2$ via the map $\overline{k-1} \mapsto (k-1) + \Delta(K)^2$. By Theorem 10.20 applied to the group K , we know that $\Delta(K)/\Delta(K)^2 \cong K/K'$ via the map $(k-1) + \Delta(K)^2 \mapsto K'k$. The map in the statement of the corollary is the composition of these two isomorphisms. ■

We are interested in the transfer homomorphism $v : G \rightarrow K/K'$, where $K \subseteq G$. Since $K/K' \cong \overline{\Delta(K)}$ in the notation of Corollary 10.23, we can ask which subgroup of $\overline{\Delta(K)}$ corresponds to $v(G)$ under this isomorphism. If $V : G \rightarrow K$ is a pretransfer map, then $v(G)$ is the image of $V(G)$ in K/K' . The subgroup of $\overline{\Delta(K)}$ corresponding to $v(G)$, therefore, is exactly the set of elements of the form $\overline{V(g) - 1}$ for $g \in G$. We shall be able to give a useful description of this subgroup in the case where K is normal in G .

Assume now that $K \triangleleft G$. If $g \in G$, then conjugation by g defines an automorphism of K , and hence $g^{-1}\Delta(K)g = \Delta(K)$. Then $\Delta(K)g = g\Delta(K)$, and since $g\Delta(G) = \Delta(G)$, we have $g\Delta(K)\Delta(G) = \Delta(K)g\Delta(G) = \Delta(K)\Delta(G)$, and thus the additive group $\Delta(K)\Delta(G)$ is invariant under left multiplication by elements of G . This subgroup of $\mathbb{Z}[G]$, therefore, is a left ideal. (It is also a right ideal, but we shall not need that fact.) Of course, $\Delta(G)$ is also a left ideal, and thus $\overline{\Delta(G)} = \Delta(G)/\Delta(K)\Delta(G)$ is a left $\mathbb{Z}[G]$ -module. Clearly, $\overline{\Delta(G)}$ is annihilated by left multiplication by elements of $\Delta(K)$, and thus $(k-1)\bar{\alpha} = 0$ for $\alpha \in \Delta(G)$ and $k \in K$. Then $k\bar{\alpha} = \bar{\alpha}$, and since the action of K is trivial, we have a left action of G/K on $\overline{\Delta(G)}$.

Now let T be a transversal for K in G , and note that since we are assuming that K is normal, there is no distinction between left and right transversals. Let $\sigma \in \mathbb{Z}[G]$ be the sum of the elements of T , and observe that left multiplication by σ defines a homomorphism of additive groups $\Xi : \overline{\Delta(G)} \rightarrow \overline{\Delta(G)}$. Also, since left multiplication by elements of K fixes all elements of $\overline{\Delta(G)}$, the map Ξ is independent of the transversal T .

10.24. Theorem. *Let $v : G \rightarrow K/K'$ be the transfer homomorphism, where G is a finite group and $K \triangleleft G$. Working in $\mathbb{Z}[G]$, write*

$$\overline{\Delta(G)} = \frac{\Delta(G)}{\Delta(K)\Delta(G)},$$

and let $\Xi : \overline{\Delta(G)} \rightarrow \overline{\Delta(G)}$ be the map defined by left multiplication by the sum of the elements of a transversal for K in G . Then $v(G) \cong \Xi(\overline{\Delta(G)})$.

Proof. Let $V : G \rightarrow K$ be a pretransfer map, so that

$$V(g) = \prod_{t \in T} tg(t \cdot g)^{-1},$$

where T is some transversal for K in G , and the product is taken in some fixed but unspecified order. Then $V(g) \in K$, and so $\overline{V(g) - 1} \in \overline{\Delta(K)}$. Under the isomorphism between $\overline{\Delta(K)}$ and K/K' in Corollary 10.23, this element corresponds to the image of $V(g)$ in K/K' , which is $v(g)$.

We argue next that

$$\overline{V(g) - 1} = \Xi(\overline{g - 1}).$$

To see this, write $tg = k_t(t \cdot g)$ for each element $t \in T$, where $k_t \in K$. Then $V(g) = \prod k_t$, and since by Corollary 10.23, the map $k \mapsto \overline{k - 1}$ is a homomorphism from K to the additive group $\overline{\Delta(K)}$, we have

$$\overline{V(g) - 1} = \sum_{t \in T} \overline{k_t - 1}.$$

Also, recall that $\Xi(\bar{\alpha}) = \sigma\bar{\alpha} = \overline{\sigma\alpha}$, where $\sigma = \sum_t t$, and thus

$$\Xi(\overline{g-1}) = \overline{\sum_{t \in T} t(g-1)}.$$

We have

$$\begin{aligned} \sum_{t \in T} t(g-1) &= \sum_{t \in T} tg - \sum_{t \in T} t \\ &= \sum_{t \in T} k_t(t \cdot g) - \sum_{t \in T} t \\ &= \sum_{t \in T} k_t(t \cdot g) - \sum_{t \in T} t \cdot g \\ &= \sum_{t \in T} (k_t - 1)(t \cdot g) \\ &\equiv \sum_{t \in T} (k_t - 1) \pmod{\Delta(K)\Delta(G)}, \end{aligned}$$

where the final congruence holds because $(k-1)x \equiv (k-1) \pmod{\Delta(K)\Delta(G)}$ for all $x \in G$ and $k \in K$. Thus

$$\Xi(\overline{g-1}) = \sum_{t \in T} \overline{k_t - 1} = \overline{V(g) - 1},$$

as claimed.

Now let X be the image of the map $g \mapsto \overline{V(g) - 1}$ from G to $\overline{\Delta(K)}$. Then X corresponds to $v(G)$ under the isomorphism of Lemma 10.23 between $\overline{\Delta(K)}$ and K/K' , and it follows that X is a subgroup. The map Ξ is a homomorphism from $\overline{\Delta(G)}$ into itself, and we have shown that Ξ carries the generators $\overline{g-1}$ of $\overline{\Delta(G)}$ onto the subgroup X . It follows that $\Xi(\overline{\Delta(G)}) = X \cong v(G)$, as wanted. ■

Recall that the assertion of Theorem 10.18 is that the transfer homomorphism $v : G \rightarrow G'/G''$ is always trivial. Actually, something a little more general is true.

10.25. Theorem. *Let G be a finite group, and let $v : G \rightarrow K/K'$ be the transfer homomorphism, where $G' \subseteq K \subseteq G$. Then $v(g)^{|K:G'|} = 1$ for all elements $g \in G$.*

Of course, if $K = G'$, then Theorem 10.25 asserts that $v(g) = 1$ for all $g \in G$, and so Theorem 10.18 is an immediate consequence. To prove Theorem 10.25, we need the following general result about modules for commutative rings.

10.26. Theorem. *Let A be a left R -module, where R is a commutative ring, and let $U \subseteq R$ be an ideal. Assume that A and U are finitely generated as*

additive groups, and suppose that UA has finite index m in A . Then there exists an element $r \in R$ such that $rA = 0$ and $r \equiv m \cdot 1 \pmod{U}$.

We review a bit of matrix theory before we begin the proof. If S is an $n \times n$ matrix over the commutative ring R , the **classical adjoint** T of S is the $n \times n$ matrix whose (i, j) -entry is plus-or-minus the determinant of the (j, i) -minor of S , where the sign is $(-1)^{i+j}$. The fact about the classical adjoint that we need is that $TS = dI$, where $d = \det(S)$ and I is the $n \times n$ identity matrix.

Proof of Theorem 10.26. By the fundamental theorem of abelian groups, the finite abelian group A/UA of order m is a direct product of cyclic subgroups C_i for $1 \leq i \leq k$. Write $m_i = |C_i|$, and observe that $m = |A/UA| = \prod m_i$. Now choose elements $a_i \in A$ such that a_i generates C_i modulo UA , and let $B = \langle a_i \mid 1 \leq i \leq k \rangle$, so that $A = B + UA$.

Next, we expand the set $\{a_i \mid 1 \leq i \leq k\}$ to obtain an appropriate generating set for A . To do this, we observe that UA is finitely generated as an additive group since both U and A are finitely generated, and so we can choose a finite generating set X for UA . Choose notation so that $X = \{a_i \mid k < i \leq n\}$, where $n = k + |X|$, and observe that since $A = B + UA$, the set $\{a_i \mid 1 \leq i \leq n\}$ generates A . Let $m_i = 1$ for $k < i \leq n$ and note that $\prod_{i=1}^n m_i = m$ and $m_i a_i \in UA$ for $1 \leq i \leq n$.

Since $m_i a_i \in UA$ for $1 \leq i \leq n$ and A is generated by the elements a_j for $1 \leq j \leq n$, we can write

$$m_i a_i = \sum_{j=1}^n s_{i,j} a_j$$

where $s_{i,j} \in U$, and we let S be the $n \times n$ matrix over R with (i, j) -entry equal to $s_{i,j}$. Also, let M be the diagonal $n \times n$ matrix with (i, i) -entry equal to $m_i \cdot 1$, and finally, let v be the $n \times 1$ column vector with entry i equal to a_i . We thus have $Mv = Sv$, and thus $(M - S)v = 0$.

Now let T be the classical adjoint of the $n \times n$ matrix $M - S$ over R . Then $T(M - S) = rI$, where $r = \det(M - S)$ and I is the $n \times n$ identity matrix over R , and we have

$$0 = T(M - S)v = rIv = rv,$$

and thus $ra_i = 0$ for $1 \leq i \leq n$. Since the elements a_i generate A , we have $rA = 0$, as required. Also, the entries of S lie in U , so we have

$$r = \det(M - S) \equiv \det(M) = \left(\prod_{i=1}^n m_i \right) \cdot 1 = m \cdot 1 \pmod{U},$$

and the proof is complete. ■

We return now to group rings of finite groups. Recall that if $K \triangleleft G$ then $\overline{\Delta(G)} = \Delta(G)/\Delta(K)\Delta(G)$ is a left $\mathbb{Z}[G]$ -module.

10.27. Lemma. *Let $K \triangleleft G$, where G is a finite group. In $\mathbb{Z}[G]$, let*

$$\overline{\Delta(G)} = \frac{\Delta(G)}{\Delta(K)\Delta(G)},$$

and let $\Xi : \overline{\Delta(G)} \rightarrow \overline{\Delta(G)}$ be the map induced by left multiplication by the sum of the elements of a transversal for K in G . Suppose that $e \in \mathbb{Z}[G]$ satisfies $e\overline{\Delta(G)} = 0$, and let $m = \delta(\epsilon)$, where δ is the augmentation map. Then $|G : K|$ divides m , and $(m/|G : K|) \cdot \Xi(\overline{\Delta(G)}) = 0$.

Proof. Let T be a transversal for K in G with $1 \in T$, and let $\sigma = \sum_t t$, so that $\Xi(\overline{\alpha}) = \sigma\overline{\alpha} = \overline{\sigma\alpha}$ for $\alpha \in \Delta(G)$. Given $t \in T$, we know that the left-multiplication maps on $\overline{\Delta(G)}$ by all elements of the coset Kt are equal, and thus it is no loss to assume that

$$\epsilon = \sum_{t \in T} e_t t$$

for some integers e_t with $\sum_t e_t = m$. If $g \in G$, then since $\epsilon\overline{\Delta(G)} = 0$, we have

$$\left(\sum_{t \in T} e_t t\right)(g - 1) \equiv 0 \pmod{\Delta(K)\Delta(G)}.$$

Now for $t \in T$, write $tg = k_t(t \cdot g)$, where $k_t \in K$. Then

$$\begin{aligned} \left(\sum_{t \in T} e_t t\right)(g - 1) &= \sum_{t \in T} e_t k_t(t \cdot g) - \sum_{t \in T} e_t t \\ &= \sum_{t \in T} e_t k_t(t \cdot g) - \sum_{t \in T} e_{t \cdot g}(t \cdot g) \\ &= \sum_{t \in T} (e_t k_t - e_{t \cdot g} 1)(t \cdot g), \end{aligned}$$

and by the previous paragraph, this element lies in $\Delta(K)\Delta(G)$. Now the $(t \cdot g)$ -component of this element with respect to T is $e_t k_t - e_{t \cdot g} 1$, and by Lemma 10.21, this component must lie in $\Delta(K)$. It follows that $e_t - e_{t \cdot g} = 0$ for all $t \in T$ and $g \in G$.

Since the dot action of G is transitive on T , the numbers e_t must all be equal, say to e , and thus $\epsilon = e\sigma$. Also, $m = \sum e_t = e|T| = e|G : K|$, and thus $|G : K|$ divides m , as wanted. Finally, if $\alpha \in \Delta(G)$, we have

$$(m/|G : K|) \cdot \Xi(\overline{\alpha}) = e\sigma\overline{\alpha} = \epsilon\overline{\alpha} = 0,$$

and the proof is complete. ■

Proof of Theorem 10.25. As usual, write $\overline{\Delta(G)} = \Delta(G)/\Delta(K)\Delta(G)$, and observe that $K \triangleleft G$ since $G' \subseteq K$. Let $\Xi : \overline{\Delta(G)} \rightarrow \overline{\Delta(G)}$ be the (uniquely determined) map induced by left multiplication by the sum in $\mathbb{Z}[G]$ of the elements of an arbitrary transversal for K in G . By Theorem 10.24, the transfer image $v(G)$ is isomorphic to $\Xi(\overline{\Delta(G)})$, and so to show that $v(g)^{|K:G'|} = 1$ for all g in G , it suffices to show that the map $|K : G'| \Xi$ is identically zero on $\overline{\Delta(G)}$.

Write $A = \overline{\Delta(G)}$, and recall that K acts trivially (by left multiplication) on A , and thus the abelian group G/K acts on A by left multiplication, and so A is naturally a left module for the commutative ring $R = \mathbb{Z}[G/K]$. We want to apply Theorem 10.26 with $U = \Delta(G/K)$, and so we must compute the index $|A : UA|$.

We argue that $|A : UA| = |G : G'|$. To see this, observe that the action of an element $Kg \in G/K$ on A is just the action of g on A , and thus

$$UA = \Delta(G/K)A = \sum_{Kg \in G/K} ((Kg) - 1)A = \sum_{g \in G} (g - 1)A = \Delta(G)A.$$

Also,

$$\Delta(G)A = \Delta(G)\overline{\Delta(G)} = \overline{\Delta(G)^2},$$

and thus

$$|A : UA| = |\overline{\Delta(G)} : \overline{\Delta(G)^2}| = |\Delta(G) : \Delta(G)^2| = |G : G'|,$$

where the second equality holds because $\Delta(K)\Delta(G) \subseteq \Delta(G)^2$, and the third holds by Theorem 10.20.

Theorem 10.26 applies since A and $\Delta(G/K)$ are finitely generated, and it follows that there exists an element $\gamma \in \mathbb{Z}[G/K]$ such that $\gamma A = 0$ and $\gamma \equiv |G : G'| \cdot 1 \pmod{\Delta(G/K)}$. Observe that this congruence modulo $\Delta(G/K)$ implies that the augmentation of γ in the group ring $\mathbb{Z}[G/K]$ is equal to $|G : G'|$.

Since the element Kg of G/K acts on A as g does, we can use γ to construct an element $\epsilon \in \mathbb{Z}[G]$ that acts on A as γ does, and for which the augmentation is equal to the augmentation of γ , namely $|G : G'|$. Thus $\epsilon A = 0$ and $\delta(\epsilon) = |G : G'|$, and therefore Lemma 10.27 guarantees that $(|G : G'|/|G : K|)\Xi$ is identically zero on $\overline{\Delta(G)}$. Since $|G : G'|/|G : K| = |K : G'|$, we are done. ■

We close with an application of Theorem 10.18, originally proved by J. Alperin and T. Kuo with a different proof.

10.28. Corollary. *Let G be a finite group, and let $A = G' \cap \mathbf{Z}(G)$. Then $g^{|G:A|} = 1$ for all elements $g \in G$.*

Proof. Let $V : G \rightarrow A$, $U : G \rightarrow G'$ and $W : G' \rightarrow A$ be pretransfer maps, and let $g \in G$. Since A is abelian, V is actually the transfer homomorphism from G to A and W is the transfer homomorphism from G' to A . Now $A \subseteq \mathbf{Z}(G)$, and thus $V(g) = g^{|G:A|}$ by Theorem 5.6. By Theorem 10.8, which is the transitivity of transfer theorem, and again using the fact that A is abelian, we have $V(g) = W(U(g))$. Now Theorem 10.18 tells us that $U(g) \in G''$, and thus $U(g) \in \ker(W)$. We now have $g^{|G:A|} = V(g) = W(U(g)) = 1$, as wanted. ■

Problems 10C

10C.1. Let $\varphi : G \rightarrow H$ be a group homomorphism. Show that φ can be extended to a ring homomorphism $\theta : \mathbf{Z}[G] \rightarrow \mathbf{Z}[H]$, and show that $\Delta(N)\mathbf{Z}[G] = \ker(\theta) = \mathbf{Z}[G]\Delta(N)$, where $N = \ker(\varphi)$.

10C.2. Let A be an additively written finitely generated free abelian group. Show that all \mathbf{Z} -bases for A have the same finite size.

Hint. Let p be a prime number and let $B = pA$. Show that A/B is a finite dimensional vector space over the field F of order p .

10C.3. Let H be a subgroup of the group U of invertible elements in $\mathbf{Z}[G]$, and suppose that H is a \mathbf{Z} -basis for the additive group of $\mathbf{Z}[G]$. Show that there is a subgroup $K \subseteq U$ such that $K \cong H$ and K is also a \mathbf{Z} -basis for $\mathbf{Z}[G]$, and such that $\delta(k) = 1$ for all elements $k \in K$, where δ is the augmentation map on $\mathbf{Z}[G]$.

Note. It had been conjectured that in this situation, H and G were necessarily isomorphic, but this is now known to be false,

10C.4. As in the previous problem, let H be a \mathbf{Z} -basis for $\mathbf{Z}[G]$, where H is a subgroup of the group U of invertible elements in $\mathbf{Z}[G]$. Show that $G/G' \cong H/H'$.

10C.5. Let $|G| = n$ and suppose that the elements of G are numbered, so that $G = \{g_1, g_2, \dots, g_n\}$. Given an element $\alpha \in \mathbf{Z}[G]$, let $M(\alpha)$ be the $n \times n$ matrix over \mathbf{Z} whose (i, j) -entry is equal to the coefficient of g_j in $g_i \alpha$. Show that the trace $\text{tr}(M(\alpha))$ is ne , where $e \in \mathbf{Z}$ is the coefficient of 1 in α .

10C.6. In the situation of the previous problem, suppose that $\alpha^m = 1$ for some integer m . Show that all eigenvalues of the matrix $M(\alpha)$ are roots of unity, and deduce that $e \in \{-1, 0, 1\}$.

Hint. Show that $M(\alpha)^m$ is the identity matrix, and use the fact that the trace of an $n \times n$ matrix is equal to the sum of its n eigenvalues, counting multiplicities.

Appendix: The Basics

In this appendix, we provide a quick review of some of the basic facts of elementary group theory that are assumed in the foregoing chapters. The presentation here is neither detailed nor exhaustive, however, and readers may wish to consult the appropriate sections of a general abstract-algebra text for a more comprehensive treatment of some of this material. (Parts of our book *Algebra: A Graduate Course*, for example, would be a good supplementary source for the theory needed here.)

A **group** is a set G together with an associative binary operation on G that satisfies two further conditions: there must be a (two-sided) identity element in G , and each element of G must have a (two-sided) inverse with respect to that identity. We generally write our groups multiplicatively, denoting the identity by the symbol “1”, and writing “ x^{-1} ” for the inverse of an element $x \in G$. (It makes sense to fix this notation because, as is easy to check, a group G has a unique identity, and each element $x \in G$ has a unique inverse.)

A group that plays a fundamental role in the theory is the **symmetric group** on a nonempty set X . This group, denoted $\text{Sym}(X)$, is the set of all bijections from X onto itself, and the binary “multiplication” in $\text{Sym}(X)$ is function composition. (The elements of $\text{Sym}(X)$ are also referred to as **permutations** of X .) The group identity in $\text{Sym}(X)$ is the identity map on X , and this explains why the identity of a group is called the “identity” element. (Note that in this book, we compose functions from left to right, so that if $\alpha, \beta \in \text{Sym}(X)$, then $\alpha\beta$ means “do α , then β ”, and so we can write $(x)(\alpha\beta) = ((x)\alpha)\beta$.) In the case where $X = \{1, 2, \dots, n\}$ we write S_n for $\text{Sym}(X)$, and we note that $|S_n| = n!$.

A **transposition** in $\text{Sym}(X)$ is a permutation that interchanges two points, leaving all other members of X fixed, and it is not hard to see that every permutation is a product of transpositions. Less trivial is the fact that if $\alpha \in \text{Sym}(X)$ is written as a product of r transpositions, then although the integer r is not uniquely determined by α , its parity is. In other words, either every representation of α as a product of transpositions involves an even number of transpositions, or else every such representation involves an odd number of transpositions. Exactly half of the permutations on a set X containing at least two points are products of an even number of transpositions, and these **even** permutations form a group called the **alternating group** on X , denoted $\text{Alt}(X)$. If $X = \{1, 2, \dots, n\}$, we write A_n for $\text{Alt}(X)$, and we note that $|A_n| = (n!)/2$.

Now let $x \in G$, where G is an arbitrary group. If n is an integer, we define x^n as follows. If $n > 0$, then $x^n = xx \cdots x$ is the product of n copies of x ; if $n < 0$, then, of course, $-n$ is positive, and we define $x^n = (x^{-1})^{-n}$, and finally, we set $x^0 = 1$. With these definitions, it is easy to check that $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$ for all integers $m, n \in \mathbb{Z}$.

In group theory, the word “order” has two different, but not entirely unrelated meanings. The **order** of a group G is its cardinality, denoted $|G|$, and the **order** of an element $x \in G$, denoted $o(x)$, is the smallest positive integer n such that $x^n = 1$. (If there is no such positive integer, we say that x has **infinite order**.) If $o(x) = n$, then for integers a and b , we have $x^a = x^b$ if and only if $a \equiv b \pmod{n}$, and thus there are precisely n different elements of G that are powers of x , and it follows that $|G| \geq o(x)$. If x has infinite order, then the only way to get $x^a = x^b$ is for $a = b$, and so in this case, all of the elements x^a with $a \in \mathbb{Z}$ are distinct. In particular, if x has infinite order, there are infinitely many different powers of x , and thus G must have infinite order.

A **subgroup** of a group G is a subset $H \subseteq G$ such that H is a group in its own right, using the multiplication in G . If H is a subgroup, it is easy to check that its identity must be the identity of G , and the inverse in H of an element $x \in H$ is the inverse of x in G . A subgroup of G , therefore, is a nonempty subset that is closed under multiplication and inverses, and it is easy to see that conversely, every such subset is a subgroup. If $x \in G$ has finite order $n > 1$, then $x^{-1} = x^{n-1}$ is a power of x , and so if G is finite, it follows that it suffices to check that a nonempty subset is closed under multiplication in order to establish that it is a subgroup; closure under inverses then follows automatically.

The primary objects of interest in group theory are the subgroups of a given group G , so it is almost always the case that when we mention some

subset of G , we are thinking of a subgroup. If we write “let $H \subseteq G$ ”, therefore, then although we may neglect to say so, we generally intend that H should be a subgroup, and we do not use any special notation to denote subgroups. (For clarity, however, especially in statements of theorems, we will often not rely on this default, and we will say explicitly that H is subgroup.) In situations where we want to consider subsets that may not be subgroups, we indicate that by writing something like “let $X \subseteq G$ be a subset”.

Of course, a set that we *construct* should not automatically be assumed to be a subgroup. For example, given subsets $X, Y \subseteq G$, the subset XY is defined by $XY = \{xy \mid x \in X, y \in Y\}$. But even if X and Y are subgroups, it is not generally true that XY is a subgroup.

X.1. Lemma. *Let H and K be subgroups of a group G . Then HK is a subgroup if and only if $HK = KH$.*

Proof. If $HK = KH$, then $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$, and thus HK is closed under multiplication. Also, if $h \in H$ and $k \in K$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, and hence HK is closed under inverses. Since $1 \in HK$, we see that HK is nonempty, and thus it is a subgroup. Conversely, suppose that HK is a subgroup. Then $K \subseteq HK$ and $H \subseteq HK$, and since HK is closed under multiplication, we have $KH \subseteq HK$. To prove the reverse containment, let $x \in HK$. Since HK is closed under inverses, we have $x^{-1} \in HK$, and thus we can write $x^{-1} = hk$, with $h \in H$ and $k \in K$. Then $x = (hk)^{-1} = k^{-1}h^{-1} \in KH$, and this completes the proof. ■

There is a simple formula for the cardinality of HK . (We do not say “order” since HK may not be a group.)

X.2. Lemma. *Let H and K be finite subgroups of a group G . Then $|HK| = |H||K|/|H \cap K|$.*

Proof. Write $D = H \cap K$. The set $H \times K$ of ordered pairs (h, k) with $h \in H$ and $k \in K$ has cardinality $|H||K|$, and we have a map $\theta : H \times K \rightarrow HK$ defined by $\theta((h, k)) = hk$. To complete the proof, it suffices to show that each element $x \in HK$ has exactly $|D|$ preimages with respect to θ . To see this, write $x = hk$ with $h \in H$ and $k \in K$. If $d \in D$, then also $d^{-1} \in D$ since both H and K are closed under inverses, and thus $(hd, d^{-1}k) \in H \times K$ and $\theta((hd, d^{-1}k)) = hk = x$. The pairs $(hd, d^{-1}k)$ are distinct for distinct elements $d \in D$, and this yields $|D|$ preimages for x . To see that we have all possible preimages, suppose that $\theta((h', k')) = x$ with $h' \in H$ and $k' \in K$. Then $hk = x = h'k'$, and thus $k(k')^{-1} = h^{-1}h'$, and this element, which we call d , lies in $H \cap K = D$. We have $h^{-1}h' = d$, so $h' = hd$, and also,

$d = k(k')^{-1}$, so $k' = d^{-1}k$. In other words, (h', k') is one of the preimages that we have already constructed, and the proof is complete. ■

The following is another useful fact about products of two subgroups.

X.3. Lemma (Dedekind). *Let H and K be subgroups of a group G , and let $H \subseteq U \subseteq G$, where U is also a subgroup. Then $HK \cap U = H(K \cap U)$.*

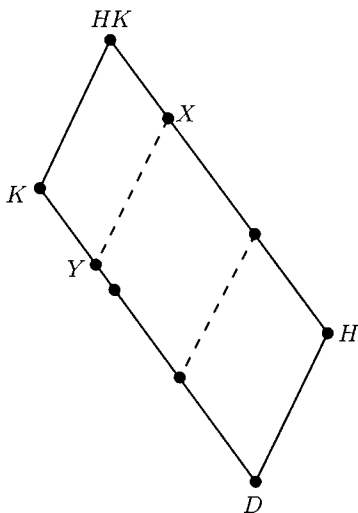
Proof. It is clear that $H(K \cap U) \subseteq HK$, and since $H \subseteq U$, we also have $H(K \cap U) \subseteq U$. Thus $H(K \cap U) \subseteq HK \cap U$, and it suffices to prove the reverse containment. Let $u \in HK \cap U$, and write $u = hk$, with $h \in H$ and $k \in K$. Then $k = h^{-1}u \in U$ since $H \subseteq U$ and $u \in U$. Thus $k \in U$, and we have $k \in K \cap U$, and so $u = hk \in H(K \cap U)$, and the proof is complete. ■

The following shows how Dedekind's lemma can be used. Before stating the result, however, we mention that intersections of arbitrary collections of subgroups are always subgroups. (This is clear since intersections of subgroups are closed under multiplication and inverses, and they contain the identity, so they cannot be empty.)

X.4. Corollary. *Suppose that H and K are subgroups of a group G , and assume that HK is also a subgroup. Let $D = H \cap K$, and let \mathcal{X} and \mathcal{Y} be the collections of subgroups defined by*

$$\mathcal{X} = \{X \mid H \subseteq X \subseteq HK\} \quad \text{and} \quad \mathcal{Y} = \{Y \mid D \subseteq Y \subseteq K\}.$$

Define the map $\theta : \mathcal{X} \rightarrow \mathcal{Y}$ by intersection with K , so that $\theta(X) = X \cap K$. Then θ is injective, and its image is the set $\mathcal{W} = \{W \in \mathcal{Y} \mid WH = HW\}$.



In the diagram, the parallelogram formed by K , HK , H and D is a **direct diamond**, which means that the lower node corresponds to the intersection of the subgroups represented by the side nodes, and the upper node corresponds to their product. The members of \mathcal{X} lie along the upper edge, joining H and HK , and the members of \mathcal{Y} lie along the parallel lower edge. The dashed lines represent the map θ , so that, for example, $\theta(X) = Y$. In fact, each dashed line divides the original figure into two new direct diamonds. For example, the upper parallelogram formed by the dashed line joining X to Y is a direct diamond because $X \cap K = Y$ and (as should be clear) $XK = HK$. The parallelogram formed by Y , X , H and D is also a direct diamond because $H \cap Y = D$ and $HY = X$, where as we shall see in the proof, the latter equality is a consequence of Dedekind's lemma. The node on the lower edge that is not joined to a corresponding node on the upper edge is intended to represent the fact that the map θ need not be surjective.

Proof of Corollary X.4. It should be clear that intersection with K actually does define a map from \mathcal{X} to \mathcal{Y} . Now let $X \in \mathcal{X}$. Then $H \subseteq X \subseteq HK$, and therefore $X = X \cap HK = H(X \cap K) = H\theta(X)$, where the second equality follows by Dedekind's lemma, which applies since $H \subseteq X$. This shows that X is determined by its image $\theta(X)$, and thus θ is injective. Also, since $H\theta(X) = X$ is a subgroup, it follows by Lemma X.1 that $\theta(X)H = X\theta(U)$, and thus $\theta(X) \in \mathcal{W}$. Finally, if $W \in \mathcal{W}$, then WH is a group by Lemma X.1, and since $W \subseteq K$, we have $WH \in \mathcal{X}$. Now $\theta(WH) = WH \cap K = W(H \cap K) = W$, where the second equality follows by Dedekind's lemma and the third equality holds because $H \cap K \subseteq W$. ■

Let G be an arbitrary group. If $g \in G$, the subset $G = \{g^n \mid n \in \mathbb{Z}\}$ is easily seen to be a subgroup, and clearly, G is contained in every subgroup of G that contains g . We can thus describe G as the unique smallest subgroup of G that contains g , where "smallest" should be understood in the sense of containment. In fact, if X is an *any* subset of G , there is a unique smallest subgroup that contains X , namely the intersection of all of the subgroups of G that contain X . (This makes sense because there certainly is at least one subgroup of G containing X , namely G itself, and in general, intersections of subgroups are subgroups.) The unique smallest subgroup of G that contains X is said to be the subgroup **generated** by X , and it is denoted $\langle X \rangle$.

A **maximal** subgroup of a group G is a proper subgroup M such that there is no subgroup H with $M < H < G$. (It is clear that every proper subgroup of a finite group is contained in at least one maximal subgroup,

but some infinite groups, for example the additive group of the real numbers, have no maximal subgroups at all.) The intersection of all of the maximal subgroups of a finite group G is the **Frattini** subgroup, denoted $\Phi(G)$. An interesting property of $\Phi(G)$ is that it is exactly the set of elements of G that cannot contribute to the construction of a generating set for G .

X.5. Lemma. *Let G be a finite group. If $X \subseteq G$ is a subset such that $\langle X \rangle < G$, then also $\langle X \cup \Phi(G) \rangle < G$. Conversely, if $u \in G$ has the property that whenever $\langle X \rangle < G$, also $\langle X \cup \{u\} \rangle < G$, then $u \in \Phi(G)$.*

Proof. Let $X \subseteq G$ be a subset such that $\langle X \rangle < G$. Then $\langle X \rangle$ is contained in some maximal subgroup M of G , and since also $\Phi(G) \subseteq M$, we see that $X \cup \Phi(G) \subseteq M$, and thus $\langle X \cup \Phi(G) \rangle \subseteq M < G$.

Now suppose that $u \in G$ is an element such that $\langle X \cup \{u\} \rangle < G$ for all subsets X of G such that $\langle X \rangle < G$. To prove that $u \in \Phi(G)$, we must show that $u \in M$ for all maximal subgroups M of G , so suppose $u \notin M$, where M is a maximal subgroup. Then $\langle M \rangle = M < G$, and hence $\langle M \cup \{u\} \rangle < G$, by hypothesis. We have $M < \langle M \cup \{u\} \rangle < G$, and this is a contradiction since M is a maximal subgroup. ■

We have seen that a subgroup $G = \langle g \rangle$ generated by a single element $g \in G$ is exactly the set of powers of g in G . (A group generated by a single element is said to be cyclic.) If $o(g)$ is finite, the elements g^i are distinct for $0 \leq i < o(g)$, and since these are easily seen to be all of the elements of G , it follows that $|C| = o(g)$ in this case. On the other hand, if g has infinite order, it is clear that G has infinite order.

If G is a cyclic group, so that $G = \langle g \rangle$ for some element $g \in G$, it is easy to describe all of the subgroups of G .

X.6. Lemma. *Let G be a cyclic group with $G = \langle g \rangle$, and let $H \subseteq G$ be a nonidentity subgroup. Then $g^m \in H$ for some positive integer m , and if m is the smallest such integer, then m divides every integer n such that $g^n \in H$. Also, $H = \langle g^m \rangle$, and in particular, all subgroups of G are cyclic.*

Proof. Since all elements of G are powers of g and H contains some nonidentity element, it follows that $g^a \in H$ for some nonzero integer a . If $a < 0$, then $g^{-a} = (g^a)^{-1} \in H$, and thus in any case, H contains an element of the form g^m with $m > 0$, and we can choose m to be as small as possible.

Suppose now that $g^n \in H$ for some integer n . By the “division algorithm” we can write $n = qm + r$, where the “remainder” r satisfies $0 \leq r < m$. We have $g^r = g^n (g^m)^{-q}$, and this element lies in H since both $g^n \in H$ and $g^m \in H$. Since $r < m$, it follows by the minimality of m that we cannot have $r > 0$, and thus $r = 0$, and m divides n , as required.

To show that $H = \langle g^m \rangle$, we must show that an arbitrary element $h \in H$ is a power of g^m . But $G = \langle g \rangle$, so we can certainly write $h = g^n$ for some integer n , and thus since $g^n \in H$, we know that n/m is an integer. Then $h = g^n = (g^m)^{n/m}$, and this completes the proof. ■

X.7. Corollary. *Let $G = \langle g \rangle$ be a finite cyclic group of order n , and for each positive divisor d of n , let $G_d = \langle g^{n/d} \rangle$. Then G_d is the unique subgroup of G having order d , and these subgroups G_d are all of the subgroups of G .*

Proof. Observe that $o(g) = |G| = n$ and $|G_d| = o(g^{n/d})$. Now $(g^{n/d})^d = g^n = 1$, and if $0 < e < d$, then $(n/d)e < n$, and so $(g^{n/d})^e \neq 1$. It follows that $o(g^{n/d}) = d$, and thus $|G_d| = d$.

We show next that an arbitrary subgroup H of G is one of the subgroups G_d . If H is trivial, it is G_1 , and so we can assume that H is nontrivial, and we let m be the smallest positive integer such that $g^m \in H$. Since $g^n = 1 \in H$, Lemma X.6 guarantees that m divides n and that $H = \langle g^m \rangle$. It follows that $H = G_d$, where $d = n/m$, and this completes the proof. ■

We have just seen that if G is a finite cyclic group and H is a subgroup, then $|H|$ divides $|G|$. In fact, this is true for all finite groups G , even if they are not cyclic. To establish this theorem of Lagrange, we consider cosets.

Given a subgroup $H \subseteq G$ and an element $x \in G$, where G is an arbitrary group, the set $Hx = \{hx \mid h \in H\}$ is a **right coset** of H in G . The number of these right cosets, which may be infinite, is the **index** of H in G , which is denoted $|G : H|$. (Of course, the index is the number of *different* right cosets of H in G . If $Hx = Hy$, then this coset with two names should be counted only once.)

X.8. Theorem (Lagrange). *Let H be a subgroup of an arbitrary group G . The following then hold.*

- (a) *Let $y \in Hx$, where $x \in G$. Then $Hy = Hx$.*
- (b) *Distinct right cosets of H in G are disjoint.*
- (c) *All right cosets of H in G have cardinality equal to $|H|$.*
- (d) *If $|G|$ is finite, then $|H|$ divides $|G|$ and $|G|/|H| = |G : H|$.*

Proof. We show first that if $h \in H$, then $Hh = H$. (Note that this is the special case of (a) where $x = 1$ and $y = h$.) Since $h^{-1} \in H$ and H is closed under multiplication, we have $Hh^{-1} \subseteq H$. Right multiplication by h yields $H \subseteq Hh$, and the reverse containment is another consequence of the fact that H is closed under multiplication. Assertion (a) follows since we can write $y = hx$, where $h \in H$, and thus $Hy = Hhx = Hx$. Now (b) is immediate since if $z \in Hx \cap Hy$, then $Hx = Hz = Hy$ by two applications of (a).

For (c), we construct a bijection $\theta : H \rightarrow Hx$, where Hx is an arbitrary right coset of H in G . Let $\theta(h) = hx$ and observe that θ is automatically surjective since by definition, every element of Hx has the form hx for some element $h \in H$. Also, θ is injective since if $hx = kx$ for elements $h, k \in H$, then right multiplication by x^{-1} yields $h = k$.

Finally, since $g \in Hg$ for all $g \in G$, we see that G is the union of the $|G : H|$ right cosets of H in G . These cosets are disjoint by (b), and each of them has cardinality $|H|$ by (c), and thus $|G| = |G : H||H|$, proving (d). ■

X.9. Corollary. *Let $g \in G$, where G is a finite group. Then $o(g)$ divides $|G|$.*

Proof. We have $o(g) = |\langle g \rangle|$, which divides $|G|$ by Lagrange's theorem. ■

The **exponent** of a finite group is the least common multiple of the orders of its elements. By Corollary X.9, therefore, the exponent of G divides $|G|$ for finite groups G .

Everything we did with right cosets works as well with **left cosets** of the form $xH = \{xh \mid h \in H\}$. In particular, the “mirror image” of Theorem X.8(d) shows that if $H \subseteq G$, where G is finite, then the number of left cosets of H in G is also equal to $|G|/|H|$, and thus the sets $\{Hx \mid x \in G\}$ and $\{xH \mid x \in G\}$ have equal cardinality (although in general, they are different sets). But even if G is infinite, the cardinalities of the sets of left and right cosets of H in G are equal. To see this, consider the bijection from the set of all subsets of G to itself defined by $X \mapsto \{x^{-1} \mid x \in X\}$, and check that it carries each left coset of H in G to a right coset and *vice versa*.

X.10. Corollary. *Let $H \subseteq K \subseteq G$, where G is a finite group and H and K are subgroups. Then $|G : H| = |G : K||K : H|$.*

Proof. Since $|G : K| = |G|/|K|$ and $|K : H| = |K|/|H|$, we conclude that $|G : K||K : H| = |G|/|H| = |G : H|$. ■

X.11. Corollary. *Let H and K be subgroups of a finite group G . Then $|K : H \cap K| \leq |G : H|$, and equality holds if and only if $HK = G$.*

Proof. Since HK is a subset of G , Lemma X.2 yields

$$|G| \geq |HK| = \frac{|H||K|}{|H \cap K|},$$

with equality if and only if $HK = G$. Then

$$|K : H \cap K| = \frac{|K|}{|H \cap K|} \leq \frac{|G|}{|H|} = |G : H|,$$

again with equality if and only if $HK = G$. ■

Another useful fact in this vein is the following.

X.12. Corollary. *Let H and K be subgroups of a finite group G , and suppose that $|G : H|$ and $|G : K|$ are relatively prime. Then $HK = G$.*

Proof. Since $H \cap K \subseteq H \subseteq G$, it follows by Corollary X.10 that $|G : H|$ divides $|G : H \cap K|$, and similarly, $|G : K|$ divides $|G : H \cap K|$. Since the indices $|G : H|$ and $|G : K|$ are coprime, their product must divide $|G : H \cap K|$, and thus

$$\frac{|G|^2}{|H||K|} = |G : H||G : K| \leq |G : H \cap K| = \frac{|G|}{|H \cap K|}.$$

This yields

$$|G : H| = \frac{|G|}{|H|} \leq \frac{|K|}{|H \cap K|} = |K : H \cap K|,$$

and thus by Corollary X.11, equality holds and $HK = G$. ■

Versions of these corollaries hold even for infinite groups, but we will not give proofs, or even precise statements.

If G_1 and G_2 are groups, a bijection $\theta : G_1 \rightarrow G_2$ is said to be an **isomorphism** if θ respects multiplication, by which we mean that $\theta(xy) = \theta(x)\theta(y)$ for all elements $x, y \in G_1$. Also, if there is an isomorphism from G_1 to G_2 , we say that the groups G_1 and G_2 are **isomorphic**, and we write $G_1 \cong G_2$. (It is trivial to check that if $\theta : G_1 \rightarrow G_2$ is an isomorphism, then also $\theta^{-1} : G_2 \rightarrow G_1$ is an isomorphism, so if $G_1 \cong G_2$, then also $G_2 \cong G_1$, and in fact, “ \cong ” is an equivalence relation.)

A group theorist would say that a group is nothing but a certain multiplication rule on a set, and that what counts is the multiplication rule, and not the set. From this point of view, we see that if the underlying set of a group is changed, but the multiplication is somehow preserved, this will not fundamentally alter the group. To a group theorist, therefore, isomorphic groups are essentially identical, and so if $G_1 \cong G_2$, then G_2 enjoys all of the “group theoretic” properties of G_1 . For example, if G_1 has exactly eight elements of order 3, then the same is true of G_2 , and if G_1 has an abelian subgroup of order 10, then so too does G_2 . (A group G is **abelian** if $xy = yx$ for all $x, y \in G$.)

Of course, isomorphic groups may look very different to someone who is not a group theorist. For example, the additive group of the real numbers is isomorphic to the multiplicative group of the positive real numbers via the map $x \mapsto e^x$. More surprisingly, the additive group of the real numbers is isomorphic to the additive group of the complex numbers. (It requires an appeal to the axiom of choice to establish the existence of such an isomorphism, however, and so it is not possible to describe an explicit map.)

The following lemma shows that for each positive integer n , there is essentially only one cyclic group of order n .

X.13. Lemma. *Let $B = \langle b \rangle$ and $C = \langle c \rangle$ be cyclic groups of the same finite order n , and let $\theta : B \rightarrow C$ be defined by $\theta(b^i) = c^i$ for all integers i . Then θ is a well defined isomorphism from B onto C .*

Proof. First, observe that $o(b) = n = o(c)$. If $b^i = b^j$, then $i \equiv j \pmod n$, and thus $c^i = c^j$, and it follows that θ is unambiguously defined. Also, θ is surjective since every element of C has the form c^j for some integer j , and since $|B| = |C| < \infty$, it follows that θ is also injective. Finally, if $x, y \in B$, write $x = b^r$ and $y = b^s$ for integers r and s . Then

$$\theta(b^r b^s) = \theta(b^{r+s}) = c^{r+s} = c^r c^s = \theta(b^r) \theta(b^s),$$

and so $\theta(xy) = \theta(x)\theta(y)$, and θ is an isomorphism. ■

If $\theta : G_1 \rightarrow G_2$ is an isomorphism, it should be clear that θ carries each subgroup of G_1 to a subgroup of G_2 , and in fact, the map $H \mapsto \theta(H)$ is a bijection from the set of subgroups of G_1 onto the set of subgroups of G_2 . Furthermore, if $H \subseteq G_1$ is a subgroup that satisfies a certain property in G_1 , then its image $\theta(H)$ satisfies the corresponding property in G_2 .

Given a group G , consider, for example, the set of elements $z \in G$ that commute with all elements of G . This set, denoted $\mathbf{Z}(G)$, is the **center** of G , and it is easy to check that it is a subgroup. If $\theta : G_1 \rightarrow G_2$ is an isomorphism, it should be clear that θ carries the center of G_1 to the center of G_2 . More generally, if H is any subgroup of G_1 that can be described with the definite article “the”, then $\theta(H)$ is the corresponding subgroup of G_2 . For example, if H is the Frattini subgroup of G_1 or the derived subgroup of G_1 , then the image $\theta(H)$ is respectively the Frattini subgroup or the derived subgroup of G_2 . (It is not necessary to know the definition of the derived subgroup to see that this must be true.)

An isomorphism from a group G to itself is called an **automorphism** of G , and the set of all automorphisms of G is denoted $\text{Aut}(G)$. Of course, $\text{Aut}(G)$ is a subset of $\text{Sym}(G)$, and it is easy to see that in fact, $\text{Aut}(G)$ is a subgroup of $\text{Sym}(G)$.

X.14. Lemma. *Let G be a cyclic group. Then $\text{Aut}(G)$ is abelian, and if G is finite, then $|\text{Aut}(G)| = \varphi(|G|)$, where φ is Euler’s totient function.*

Proof. Write $G = \langle g \rangle$. Observe first that if $\alpha, \beta \in \text{Aut}(G)$ and $\alpha(g) = \beta(g)$, then $\alpha(g^n) = \alpha(g)^n = \beta(g)^n = \beta(g^n)$ for all integers n . Since every element of G has the form g^n for some integer n , it follows that α and β agree on all of G , and thus $\alpha = \beta$.

Now let $\sigma, \tau \in \text{Aut}(G)$. Then $\sigma(g) = g^s$ and $\tau(g) = g^t$ for some integers s and t , and it is easy to check that $\sigma\tau$ and $\tau\sigma$ both carry g to g^{st} . Since $\sigma\tau$ and $\tau\sigma$ agree on g , we conclude that these automorphisms are equal, and hence $\text{Aut}(G)$ is abelian.

Now suppose $|G| = n$, so that $o(g) = n$. Since automorphisms preserve orders of elements, every automorphism of G maps g to an element of the set $X = \{x \in G \mid o(x) = n\}$, and by the first paragraph of the proof, distinct automorphisms of G carry g to distinct elements of X . If $x \in X$ is arbitrary, then $G = \langle x \rangle$, and hence by Lemma X.13, there is an isomorphism θ from $G = \langle g \rangle$ to $G = \langle x \rangle$ such that $\theta(g) = x$. Thus θ is an automorphism of G that carries g to x , and it follows that $|\text{Aut}(G)| = |X|$.

To complete the proof, we argue that $|X| = \varphi(n)$. Since every element of G is uniquely of the form g^r with $0 \leq r < n$, it suffices to show that $g^r \in X$ if and only if r and n are coprime. To see this, let $H = \langle g^r \rangle$, so that $|H| = o(g^r)$, and let m be the unique smallest positive integer such that $g^m \in H$. It follows by Lemma X.6, that m divides both r and n , and thus if r and n are coprime, we have $m = 1$ and $g \in H$, and thus $H = G$. Then $o(g^r) = |H| = n$, and $g^r \in X$.

Conversely, suppose that $g^r \in X$ and let m be the greatest common divisor of r and n . Write $d = n/m$, so that $n = md$, which divides rd , and thus $(g^r)^d = 1$ and $d \geq o(g^r) = n$. Then $d = n$ and $m = 1$, as wanted. ■

A subgroup $H \subseteq G$ is **characteristic** if every automorphism of G maps H onto H . Since an isomorphism from one group to another carries the center to the center and the Frattini subgroup to the Frattini subgroup, it follows that an automorphism of a group G carries $\mathbf{Z}(G)$ to $\mathbf{Z}(G)$ and $\Phi(G)$ to $\Phi(G)$. More generally, every subgroup of a group G that can be described unambiguously using the word “the” must be mapped to itself by all automorphisms of G , and hence such a subgroup is characteristic. In particular, if G is a finite cyclic group, then every subgroup of G is characteristic because if $H \subseteq G$ and $|H| = d$, then by Corollary X.7, we can say that “ H is *the* subgroup of G having order d ”.

Given elements x and g in a group G , we write x^g to denote the element $g^{-1}xg$, and we say that x^g is **conjugate** to x in G . (Note that $x^g = x$ if and only if $xg = gx$.) It is easy to see that conjugation by g is an automorphism of G . (This map is both injective and surjective because it has an inverse, namely conjugation by g^{-1} , and it is trivial to check that $(xy)^g = x^g y^g$ as required.) The automorphism $x \mapsto x^g$ is said to be an **inner** automorphism of G , and the set of all inner automorphisms of G is denoted $\text{Inn}(G)$. Since $(x^g)^h = x^{gh}$, for all $x, g, h \in G$, it is easy to see that $\text{Inn}(G)$ is a subgroup of the full automorphism group $\text{Aut}(G)$.

If $X \subseteq G$ is a subset and $g \in G$, then the image of X under conjugation by g is the subset $X^g = \{x^g \mid x \in X\}$. Since the conjugation maps are automorphisms, it follows that if $H \subseteq G$ is a subgroup, then all of its conjugates H^g for $g \in G$ are subgroups too. Now recall that a characteristic subgroup of G is a subgroup that is mapped to itself by all automorphisms of G . We can weaken this condition and consider the **normal** subgroups of G , which are those subgroups that are mapped to themselves by all *inner* automorphisms of G . A subgroup $H \subseteq G$ is normal, therefore, precisely when $H^g = H$ for all elements $g \in G$. We write $H \triangleleft G$ in this case. Of course, characteristic subgroups are automatically normal.

In general, it is not true that normal subgroups of normal subgroups of a group G are normal in G , but the following substitute is often useful.

X.15. Lemma. *Let $N \triangleleft G$, where G is a group, and let C be characteristic in N . Then $C \triangleleft G$.*

Proof. Let $g \in G$ and let σ be the inner automorphism of G defined by conjugation by g . Then σ is injective, and it maps N onto N , and since σ respects multiplication, the restriction of σ to N is an automorphism of N . As C is characteristic in N , we have $C^g = \sigma(C) = C$, and thus $C \triangleleft G$. ■

Given a subgroup $H \subseteq G$, the set $\{g \in G \mid H^g = H\}$, is the **normalizer** of H in G , which is denoted $\mathbf{N}_G(H)$. It is easy to see that $\mathbf{N}_G(H)$ is always a subgroup of G , and that it contains the subgroup H . It follows that $\mathbf{N}_G(H)$ is the unique largest subgroup of G that contains H as a normal subgroup.

Since conjugation by an element $g \in G$ is an injective map, $|H^g| = |H|$ for subgroups H of G . Thus if $|H|$ is finite and $H^g \subseteq H$, then $H^g = H$, and $g \in \mathbf{N}_G(H)$. In general, however, it can happen that H^g is proper in H . But if $H^g \subseteq H$ for *all* elements $g \in G$, then also $H^{g^{-1}} \subseteq H$. Conjugating both sides by g , we get $H \subseteq H^g$, and thus in fact, $H^g = H$. To show that $H \triangleleft G$, therefore, it suffices to check that $H^g \subseteq H$ for all elements $g \in G$.

X.16. Lemma. *Let H be a subgroup of a group G . Then the following are equivalent.*

- (1) $H \triangleleft G$.
- (2) $Hx = xH$ for all $x \in G$.
- (3) Every right coset of H in G is a left coset of H .
- (4) Every left coset of H in G is a right coset of H .
- (5) $(Hx)(Hy) = Hxy$ for all $x, y \in G$.
- (6) The set of right cosets of H in G is closed under multiplication.

Proof. It is clear that (2) implies (4). Conversely, if (4) holds and $x \in G$, then the left coset xH is a right coset of H containing x , and so it must be the coset Hx by Theorem X.8(a), and this proves (2). Thus (2) and (4) are equivalent, and since (2) is left-right symmetric, it must also be equivalent to (3), which is the mirror image of (4). Also, (5) and (6) are easily seen to be equivalent. That (5) implies (6) is obvious, and conversely, assuming that $HxHy$ is a right coset of H , then since it contains the element xy , it must be the right coset Hxy by Theorem X.8(a).

Now assume (1), so that $H \triangleleft G$, and let $x \in G$. Then $H = H^x = x^{-1}Hx$, and left multiplication by x yields $xH = Hx$, and thus (2) holds. Now assume (2), and let $x, y \in G$. Then $HxHy = H(xH)y = H(Hx)y = Hxy$ since $HH = H$, and this proves (5). To complete the proof, it suffices to show that (5) implies (1). To see this, assume (5) and let $x \in G$. Then

$$H^x = x^{-1}Hx \subseteq Hx^{-1}Hx = Hx^{-1}x = H,$$

and since this holds for all $x \in G$, we have $H \triangleleft G$. ■

A useful observation about a normal subgroup $N \triangleleft G$ is that if $H \subseteq G$ is an arbitrary subgroup, then NH is a subgroup. To see why this is so, observe that

$$NH = \bigcup_{h \in H} Nh = \bigcup_{h \in H} hN = HN,$$

and apply Lemma X.1.

Now let N be a normal subgroup of G , where G is an arbitrary group, and write G/N to denote the set of right cosets of N in G . (Of course, Lemma X.16 implies that the word “right” in the previous sentence is superfluous because for normal subgroups, there is no distinction between left cosets and right cosets.) By condition (5) of Lemma X.16, the set G/N is closed under multiplication, and we observe that in fact it is a group since the coset $N1 = N$ acts as an identity and $(Nx)(Nx^{-1}) = N1$, so that Nx^{-1} is the inverse of Nx in G/N . The group G/N is called the **quotient group** or **factor group** of G with respect to the normal subgroup N . (We stress that N must be normal; otherwise by Lemma X.16, there are right cosets whose product is not a right coset.)

If G and H are arbitrary groups, a map $\theta : G \rightarrow H$ is called a **homomorphism** if $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in G$. (Thus an isomorphism is a homomorphism that happens to be both injective and surjective.)

We consider some examples of homomorphisms. Given an arbitrary group G , let $\theta(x) \in \text{Aut}(G)$ be conjugation by x . It is trivial to check that $g^{xy} = (g^x)^y$ for elements $g, x, y \in G$, and thus $\theta(xy) = \theta(x)\theta(y)$ and $\theta : G \rightarrow \text{Aut}(G)$ is a homomorphism. (Remember that multiplication in $\text{Aut}(G)$ is defined to be left-to-right.) The image of G under θ , of course,

is $\text{Inn}(G)$. For another example, let \mathbb{Z} be the additive group of the integers and let H be an arbitrary group. Fix an element $h \in H$ and consider the map $n \mapsto h^n$ from \mathbb{Z} to H . Since $h^{m+n} = h^m h^n$ for $m, n \in \mathbb{Z}$, this map is a homomorphism, and the image of \mathbb{Z} in H is clearly the subgroup $\langle h \rangle$.

Perhaps the most important example is the **canonical** homomorphism $\pi : G \rightarrow G/N$, where $N \triangleleft G$ and $\pi(g) = Ng$. Observe that π really is a homomorphism since $\pi(xy) = Nxy = (Nx)(Ny) = \pi(x)\pi(y)$ for elements $x, y \in G$. The canonical homomorphism π is always surjective, but since all elements of N map to the identity of G/N , it is never injective unless $N = 1$, the trivial subgroup.

Given an arbitrary group homomorphism $\theta : G \rightarrow H$, the **kernel** of θ , denoted $\ker(\theta)$ is the set $\{x \in G \mid \theta(x) = 1\}$. For example, the kernel of the homomorphism $\theta : G \rightarrow \text{Aut}(G)$, where $\theta(x)$ is conjugation by x , is the set of elements $x \in G$ such that $g^x = g$ for all $g \in G$. Since $g^x = g$ if and only if $gx = xg$, we see that $\ker(\theta) = \mathbf{Z}(G)$, the center of G . For another example, consider the canonical homomorphism $\pi : G \rightarrow G/N$, where $N \triangleleft G$. Since the identity of G/N is the coset N , we see that g lies in $\ker(\pi)$ precisely when $Ng = N$, and thus $\ker(\pi) = N$.

X.17. Lemma. *Let $\theta : G \rightarrow H$ be a group homomorphism, and let $N = \ker(\theta)$. The following then hold.*

- (a) $\theta(1) = 1$.
- (b) $\theta(x^{-1}) = \theta(x)^{-1}$ for $x \in G$.
- (c) N is a normal subgroup of G .
- (d) For $x, y \in G$, we have $\theta(x) = \theta(y)$ if and only if $Nx = Ny$.
- (e) θ is injective if and only if $N = 1$.

Proof. We have $\theta(1)\theta(1) = \theta(1 \cdot 1) = \theta(1)$, and left multiplication by $\theta(1)^{-1}$ in H yields $\theta(1) = 1$, proving (a). Also, if $x \in G$, we have $1 = \theta(1) = \theta(xx^{-1}) = \theta(x)\theta(x^{-1})$, and (b) follows by left multiplication by $\theta(x)^{-1}$.

Now N is nonempty since $1 \in N$ by (a). Also, if $x, y \in N$, then $\theta(xy) = \theta(x)\theta(y) = 1 \cdot 1 = 1$, and thus $xy \in N$, and N is closed under multiplication. Furthermore, if $x \in N$, then $\theta(x^{-1}) = \theta(x)^{-1} = 1^{-1} = 1$, and thus $x^{-1} \in N$, and this proves that N is a subgroup. To complete the proof of (c), let $n \in N$ and $g \in G$. Then $\theta(n^g) = \theta(g^{-1}ng) = \theta(g)^{-1}\theta(g) = 1$, and hence $n^g \in N$. This shows that $N^g \subseteq N$ for all $g \in G$, and thus $N \triangleleft G$, proving (c).

For (d), observe that $\theta(x)\theta(y)^{-1} = \theta(xy^{-1})$. The left side is equal to 1 if and only if $\theta(x) = \theta(y)$, and the right side is 1 if and only if $xy^{-1} \in N$, or equivalently, $x \in Ny$, and this, we know, is equivalent to $Nx = Ny$. This proves (d), and (e) is an immediate consequence. ■

Thus kernels of homomorphisms defined on a group G are normal subgroups. Since we saw previously that every normal subgroup $N \triangleleft G$ is the kernel of the canonical homomorphism $G \rightarrow G/N$, it follows that the normal subgroups of G are exactly the kernels of the homomorphisms defined on G .

The following homomorphism theorem asserts that an arbitrary surjective homomorphism θ is essentially the canonical homomorphism from G onto G/N , where $N = \ker(\theta)$.

X.18. Theorem (Homomorphism). *Let $\theta : G \rightarrow H$ be a surjective group homomorphism, and let $N = \ker(\theta)$. Then $G/N \cong H$. In fact, there is an isomorphism $\tau : G/N \rightarrow H$ such that $\tau(Nx) = \theta(x)$ for all $x \in G$.*

Proof. Let $x \in G$. By Lemma X.17(d), all elements of the coset Nx have the same image under θ , and this image is $\theta(x)$. We can thus unambiguously define τ on G/N by setting $\tau(Nx) = \theta(x)$, and we must show that τ is an isomorphism. First,

$$\tau(NxNy) = \tau(Nxy) = \theta(xy) = \theta(x)\theta(y) = \tau(Nx)\tau(Ny),$$

and thus τ is a homomorphism. Also, since $\tau(Nx) = \theta(x)$, we see that the image of τ is the image of θ , and since this is all of H , it follows that τ is surjective. To prove that τ is injective, it suffices to check that $\ker(\tau)$ is trivial, and so we suppose that $Nx \in \ker(\tau)$. Then $1 = \tau(Nx) = \theta(x)$, and thus $x \in \ker(\theta) = N$, and so $Nx = N$, which is the identity of G/N . ■

Actually, Theorem X.18 even tells us something about homomorphisms that are not surjective. To explain this, suppose that $\theta : G \rightarrow H$ is an arbitrary homomorphism. If $X \subseteq G$ is a subgroup, it is easy to check that the image $\theta(X)$ is a subgroup of H , and in particular, $\theta(G)$ is a subgroup of H . We can thus view θ as a surjective homomorphism from G onto $\theta(G)$, and so we can apply the homomorphism theorem to deduce that $\theta(G) \cong G/\ker(\theta)$.

As an example of how the homomorphism theorem can be used, we prove the following so-called “N/C-Theorem”. To state it, we define the **centralizer** in G of a subset $X \subseteq G$ to be the set of elements of G that commute with all elements of X . It is easy to check that this set, denoted $\mathbf{C}_G(X)$, is actually a subgroup of G .

X.19. Corollary. *Let H be a subgroup of an arbitrary group G , and write $N = \mathbf{N}_G(H)$ and $C = \mathbf{C}_G(H)$. Then $C \triangleleft N$ and N/C is isomorphic to a subgroup of $\text{Aut}(H)$.*

Proof. If $x \in N$, then $H^x = H$, and we write $\tau_x : H \rightarrow H$ to denote the map $h \mapsto h^x$. Since conjugation by x is an automorphism of G , it is easy to see that τ_x is an automorphism of H . Also, if $x, y \in N$ and $h \in H$, then $(h)\tau_x\tau_y = (h^x)^y = h^{xy} = (h)\tau_{xy}$, and thus $\tau_{xy} = \tau_x\tau_y$, and it follows that

the map $\theta : N \rightarrow \text{Aut}(H)$ defined by $\theta(x) = \tau_x$ is a homomorphism. An element $x \in H$ lies in $\ker(\theta)$ if and only if τ_x is the identity map on H , or equivalently, $h^x = h$ for all $h \in H$. But $h^x = h$ precisely when $xh = hx$, and thus $\ker(\theta) = \mathbf{C}_G(H) = C$. Then $N/C \cong \theta(N) \subseteq \text{Aut}(H)$, and the proof is complete. ■

If H is a cyclic subgroup of G , for example, then $\mathbf{N}_G(H)/\mathbf{C}_G(H)$ is an abelian group since it is isomorphic to a subgroup of $\text{Aut}(H)$, which is abelian by Lemma X.14.

Another application of the homomorphism theorem is the following.

X.20. Corollary. *Let N and H be subgroups of a group G , and suppose that $N \triangleleft G$. Then $H \cap N \triangleleft H$ and $NH/N \cong H/(H \cap N)$.*

Proof. Recall that NH is a group, and observe that the right cosets of N in NH all have the form $Nnh = Nh$, where $n \in N$ and $h \in H$. Now define $\theta : H \rightarrow NH/N$ by setting $\theta(h) = Nh$, and observe that θ is surjective, and that it is the restriction to H of the canonical homomorphism $\pi : G \rightarrow G/N$. It follows that θ is a homomorphism, and $\ker(\theta) = H \cap \ker(\pi) = H \cap N$. Thus $H \cap N \triangleleft H$ and $H/(H \cap N) \cong NH/N$ by the homomorphism theorem. ■

We have already mentioned that if $\theta : G \rightarrow H$ is an arbitrary group homomorphism and $X \subseteq G$ is a subgroup, then $\theta(X)$ is a subgroup of H . The following correspondence theorem shows that if θ is surjective, then every subgroup of H is the image of some subgroup of G . In fact, much more is true.

X.21. Theorem (Correspondence). *Let $\theta : G \rightarrow H$ be a surjective group homomorphism, and let $N = \ker(\theta)$. Then the map $X \mapsto \theta(X)$ is a bijection from the set \mathcal{X} of subgroups of G that contain N onto the set \mathcal{Y} of all subgroups of H . Furthermore, if $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ and $Y = \theta(X)$, then the following hold.*

- (a) $X = \{x \in G \mid \theta(x) \in Y\}$.
- (b) The map α defined by $Xg \mapsto \theta(Xg)$ is a bijection from the set of all right cosets of X in G onto the set of all right cosets of Y in H , and in particular, $|G : X| = |H : Y|$.
- (c) $X \triangleleft G$ if and only if $Y \triangleleft H$, and in this case, the map α of (b) is an isomorphism $G/X \cong H/Y$.

Proof. To prove that the map $X \mapsto \theta(X)$ is a bijection from \mathcal{X} onto \mathcal{Y} , it suffices to construct an inverse map from \mathcal{Y} to \mathcal{X} . Given a subgroup $Y \subseteq H$, write $\theta^{-1}(Y) = \{x \in G \mid \theta(x) \in Y\}$, so that $\theta^{-1}(Y)$ is the inverse image of

Y in G . (Caution: we are not asserting that there is a map called θ^{-1} .) It is easy to check that $\theta^{-1}(Y)$ is a subgroup of G , and since it clearly contains $\ker(\theta) = N$, we have $\theta^{-1}(Y) \in \mathcal{X}$.

We proceed now to show that the map $Y \mapsto \theta^{-1}(Y)$ from \mathcal{Y} to \mathcal{X} is the inverse of the map $X \mapsto \theta(X)$ from \mathcal{X} to \mathcal{Y} . (Assertion (a) will also follow from this.) If $Y \in \mathcal{Y}$, then clearly $\theta(\theta^{-1}(Y)) \subseteq Y$. To prove equality, let $y \in Y$ and observe that since θ is surjective, there exists an element $x \in G$ such that $\theta(x) = y$. Then $x \in \theta^{-1}(Y)$, and thus $y = \theta(x)$ lies in $\theta(\theta^{-1}(Y))$, and we have $\theta(\theta^{-1}(Y)) = Y$, as needed.

If $X \in \mathcal{X}$, then clearly $X \subseteq \theta^{-1}(\theta(X))$. To prove equality, we consider an element $g \in \theta^{-1}(\theta(X))$, and we show that $g \in X$. Certainly, $\theta(g) \in \theta(X)$, and thus there exists $x \in X$ such that $\theta(g) = \theta(x)$. It follows by Lemma X.17(d) that $Ng = Nx$, and thus $g \in Ng = Nx \subseteq X$, where the final containment holds because $N \subseteq X$ by the definition of \mathcal{X} . Thus $X = \theta^{-1}(\theta(X))$, and this shows that the maps $X \mapsto \theta(X)$ and $Y \mapsto \theta^{-1}(Y)$ are inverse bijections between \mathcal{X} and \mathcal{Y} , as required.

Now let $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$, where $Y = \theta(X)$. If $g \in G$, then $\theta(Xg) = \theta(X)\theta(g) = Y\theta(g)$, and so α really is a map from the set $\{Xg \mid g \in G\}$ to the set $\{Yh \mid h \in H\}$. Also, α is surjective since if $h \in H$, then $h = \theta(g)$ for some element $g \in G$, and thus $\alpha(Xg) = \theta(Xg) = Yh$. To prove that α is injective, suppose that $\alpha(Xa) = \alpha(Xb)$ for elements $a, b \in G$. Then $Y\theta(a) = Y\theta(b)$, and so $\theta(b) = y\theta(a)$ for some element $y \in Y$. Since $Y = \theta(X)$, we have $y = \theta(x)$ for some element $x \in X$, and thus $\theta(b) = \theta(x)\theta(a) = \theta(xa)$. It follows that $Nb = Nxa$, and since $N \subseteq X$, this coset of N is contained in both Xa and Xb , which, therefore, are not disjoint. It follows that $Xa = Xb$, and thus α is injective, and the proof of (b) is complete.

Observe that $\theta(X^g) = \theta(X)^{\theta(g)} = Y^{\theta(g)}$ for all elements $g \in G$. Now suppose that $X \triangleleft G$. Let $h \in H$, and write $h = \theta(g)$, where $g \in G$. Then $Y^h = Y^{\theta(g)} = \theta(X^g) = \theta(X) = Y$, and thus $Y \triangleleft H$. Conversely, suppose that $Y \triangleleft H$. Let $g \in G$, and observe that $N = N^g \subseteq X^g$, so that $X^g \in \mathcal{X}$. Also, $\theta(X^g) = Y^{\theta(g)} = Y = \theta(X)$, and thus $X^g = X$ since the map defined on \mathcal{X} by applying θ is injective. It follows that $X \triangleleft G$, and this shows that $X \triangleleft G$ if and only if $Y \triangleleft H$, as required.

Finally, assuming that $X \triangleleft G$ and $Y \triangleleft H$, we must show that the map $\alpha : G/X \rightarrow H/Y$ is an isomorphism. We know from (b) that α is both injective and surjective, and so it suffices to show that it is a homomorphism. This is clear, however, since if $a, b \in G$, then $\theta(XaXb) = \theta(Xa)\theta(Xb)$. ■

If $X \in \mathcal{X}$ in the notation of the correspondence theorem, then clearly $N_G(X) \in \mathcal{X}$, and we argue that $\theta(N_G(X)) = N_H(\theta(X))$. To see why this is true, observe that since the normalizer of a subgroup is the largest

subgroup in which it is normal, it suffices to show that if $U, V \in \mathcal{X}$ with $U \subseteq V$, then $U \triangleleft V$ if and only if $\theta(U) \triangleleft \theta(V)$. This follows by applying the correspondence theorem to the surjective homomorphism from V to $\theta(V)$ obtained by restricting θ to V .

Next, we apply the correspondence theorem to the canonical homomorphism $\pi : G \rightarrow G/N$, where $N \triangleleft G$. Then $\ker(\pi) = N$, so \mathcal{X} is the set of all subgroups of G that contain N . If $X \in \mathcal{X}$, then $\pi(X) = X/N$, and thus the correspondence theorem tells us that every subgroup of G/N is uniquely of the form X/N , where X is a subgroup satisfying $N \subseteq X \subseteq G$. Also, $X \triangleleft G$ if and only if $X/N \triangleleft G/N$, and in that case, $G/X \cong (G/N)/(X/N)$.

We complete our review by discussing direct products. Suppose that we are given (not necessarily distinct) groups G_i with $1 \leq i \leq r$. Let P be the set of ordered r -tuples (x_1, x_2, \dots, x_r) , and define multiplication in P componentwise, so that

$$(x_1, x_2, \dots, x_r)(y_1, y_2, \dots, y_r) = (x_1y_1, x_2y_2, \dots, x_ry_r).$$

It is trivial to check that P is a group; it is called the **external direct product** of the groups G_i , and we write $P = G_1 \times G_2 \times \dots \times G_r$.

If $1 \leq i \leq r$, let $N_i \subseteq P$ be the set of r -tuples of the form

$$(1, \dots, 1, x_i, 1, \dots, 1),$$

where the component in position i is an arbitrary element $x_i \in G_i$ and all other components are the identities of the respective groups. It is easy to see that N_i is a subgroup of P , and that $N_i \cong G_i$. Also, it should be clear that every element $x \in P$ is uniquely of the form $x = n_1n_2 \dots n_r$ with $n_i \in N_i$, and in particular, we can write $P = N_1N_2 \dots N_r$.

The elements of N_i and N_j commute if $i \neq j$, and so if $1 \leq k \leq r$, we have $N_i \subseteq \mathbf{C}_P(N_k) \subseteq \mathbf{N}_P(N_k)$ for $i \neq k$. Since N_k is also contained in $\mathbf{N}_P(N_k)$, which is a subgroup, we see that $P = N_1N_2 \dots N_r \subseteq \mathbf{N}_P(N_k)$, and thus $N_k \triangleleft P$.

Given a group G and subgroups $M_i \triangleleft G$ for $1 \leq i \leq r$, we say that G is the **internal direct product** of the normal subgroups M_i provided that every element $g \in G$ is uniquely of the form $g = m_1m_2 \dots m_r$ with $m_i \in M_i$. Thus if P is the external direct product of the abstract groups G_i , then P is also the internal direct product of the normal subgroups N_i that we defined above, with $N_i \cong G_i$.

Note that “external direct product” is a *construction* since given an arbitrary finite list of groups, one can define their external direct product. But “internal direct product” is really a *statement* about a finite collection of normal subgroups of a given group; it may be true, but it is not automatically so. Despite these differences, and at the risk of confusion, we often use the

same notation, and we write $G = M_1 \times M_2 \times \cdots \times M_r$ if G is the internal direct product of its subgroups M_i .

Given a group G and subgroups $M_i \triangleleft G$ for $1 \leq i \leq r$, suppose that $G = M_1 M_2 \cdots M_r$. The following result shows what additional information is needed to prove that $G = M_1 \times M_2 \times \cdots \times M_r$.

X.22. Theorem. *Let $G = M_1 M_2 \cdots M_r$, where G is a group and M_i is a normal subgroup for $1 \leq i \leq r$. Then $G = M_1 \times M_2 \times \cdots \times M_r$ if and only if*

$$(M_1 M_2 \cdots M_{k-1}) \cap M_k = 1$$

for all subscripts k with $1 < k \leq r$.

Proof. Suppose first that $G = M_1 \times M_2 \times \cdots \times M_r$. Let

$$x \in (M_1 M_2 \cdots M_{k-1}) \cap M_k$$

for some subscript k , and write $x = n_1 n_2 \cdots n_{k-1}$, with $n_i \in M_i$. We can then write $x = m_1 m_2 \cdots m_r$, where $m_i = n_i$ for $1 \leq i < k$, and $m_i = 1$ for $i \geq k$, and we can get a second decomposition of the element x by taking $m_i = 1$ for all subscripts i different from k and $m_k = x$. In both situations, $m_i \in M_i$ for $1 \leq i \leq r$, and thus since we are working in a direct product, the factors m_i are uniquely determined. In the first case, we had $m_k = 1$, and in the second, $m_k = x$, and thus $x = 1$.

Conversely, assume that $(M_1 M_2 \cdots M_{k-1}) \cap M_k = 1$ for $1 < k \leq r$, and suppose that $m_1 m_2 \cdots m_r = n_1 n_2 \cdots n_r$, where $m_i, n_i \in M_i$ for $1 \leq i \leq r$. We want $m_i = n_i$ for all i , and so we suppose that is not true, and we let k be the largest subscript for which $m_k \neq n_k$. Then $m_1 m_2 \cdots m_k = n_1 n_2 \cdots n_k$, and in particular, $k > 1$. We have

$$(n_1 n_2 \cdots n_{k-1})^{-1} (m_1 m_2 \cdots m_{k-1}) = (n_k)(m_k)^{-1},$$

and this element lies in $M_1 M_2 \cdots M_{k-1} \cap M_k$ since $M_1 M_2 \cdots M_{k-1}$ is a group. It follows that $(n_k)(m_k)^{-1} = 1$, which is a contradiction. ■

In particular, if $G = M_1 \times M_2 \times \cdots \times M_r$ is an internal direct product, then $M_j \cap M_k = 1$ if $j \neq k$. If $r > 2$, however, this necessary condition is definitely not sufficient in the situation of Theorem X.22.

We need an easy general fact: if M and N are normal subgroups of a group G , and $M \cap N = 1$, then all elements of M commute with all elements of N . To see this, let $m \in M$ and $n \in N$, and consider the **commutator** $[m, n]$ of m and n , which, by definition, is the element $m^{-1} n^{-1} m n$. Then $[m, n] = m^{-1} m^n$, which lies in M because $M \triangleleft G$. Also, $[m, n] = (n^{-1})^m n$, which lies in N because $N \triangleleft G$. Thus $[m, n] = 1$, and this yields $m n = n m$.

If $G = M_1 \times M_2 \times \cdots \times M_r$ is an internal direct product, we conclude that the elements of M_j commute with the elements of M_k if $j \neq k$, and

it follows easily that G is the direct product of the subgroups M_i in every possible ordering of these subgroups. Given a finite collection \mathcal{X} of normal subgroups of a group G , therefore, it is meaningful to say that G is the direct product of the members of \mathcal{X} without specifying an ordering.

We have already seen that the external direct product P of groups G_i is the internal direct product of certain subgroups $N_i \triangleleft P$, where $N_i \cong G_i$. Another connection between external and internal direct products is the following.

X.23. Lemma. *Let G be a group, and suppose that G is the internal direct product of the normal subgroups M_i for $1 \leq i \leq r$. Then G is isomorphic to the external direct product of the groups M_i .*

Proof. Let P be the external direct product of the M_i , and construct a map θ from P to G by setting

$$\theta((m_1, m_2, \dots, m_r)) = m_1 m_2 \cdots m_r.$$

Then θ is a bijection since every element of G is uniquely of the form $m_1 m_2 \cdots m_r$ with $m_i \in M_i$. To show that θ is an isomorphism, we need

$$(x_1 x_2 \cdots x_r)(y_1 y_2 \cdots y_r) = x_1 y_1 x_2 y_2 \cdots x_r y_r$$

for $x_i, y_i \in M_i$, and this is clear since x_i and y_j commute when $i > j$. ■

For an example of how this can be used, suppose that G is an internal direct product of normal subgroups, each of which has a trivial center. To prove that $\mathbf{Z}(G) = 1$, it suffices to prove that $\mathbf{Z}(P) = 1$, where P is the isomorphic group constructed as the external direct product of the factors of G . It is clear, however, that an r -tuple (m_1, m_2, \dots, m_r) is central in P if and only if each component m_i is central in its respective group, and it follows that $\mathbf{Z}(P) = 1$.

Index

- abelian Hall subgroup and π -length, 94
abelian normal subgroups all cyclic, 189
abelian Sylow subgroup intersection, 38
action, 1
 action on cosets, 3, 148
 action on subspaces of vector space, 228ff
 action on right transversal, 148
 action via automorphisms, 68
 action, Frobenius, 177ff
 action, semiregular, 177
 actions fixing prime order elements, 141ff
 additive commutator in ring, 125
 adjoint (classical) of matrix, 321
 admit (of action), 131
 Alperin, J., 55, 323
 alternating group, 34
 alternating group, definition, 326
 alternating group, Schur multiplier of, 152
 alternating group, simplicity of, 250
 arrows in transitive action, 262
 augmentation ideal, 315
 augmentation map, 314
 automorphism, definition, 334
 automorphism of symmetric group, 33, 250
 automorphism tower, 278
 automorphism, order of, 70
 axiom of choice, 333
- Baer theorem, 55
Baer trick, 142
bar convention, 23
Bartels theorem, 290
base group of wreath product, 73
basis for free abelian group, 315
Bender, H., 31, 217, 271
Berkovich, Y., 86
- binomial coefficient, 9
block (of action), 237
Bochert theorem, 246ff
Brodkey theorem, 38, 71, 74
Burnside, book of, 181, 217
Burnside orbit count, 7
Burnside $p^a q^b$ -theorem, 216ff
Burnside p -nilpotence theorem, 159
Burnside theorem, prime degree action, 240
Burnside, W., 30
- Cameron, P., 249, 285
canonical homomorphism, 338
Carter subgroup, 91
Cauchy theorem, 8, 10
Cauchy-Frobenius orbit count, 7
center of group, 2, 334
central extension, 151
central prime order elements, 174
central series, 20, 115
central subgroup, transfer to, 154
centralizer, definition, 339
Cermak-Delgado subgroup, 43
chain stabilizer, 137
character theory, 53, 59, 147, 182, 216–217
character, permutation, 236
characteristic series, π -separable, 92
characteristic subgroup, 11
characteristic subgroup, definition, 335
characteristically simple group, 277
Chermak-Delgado theorem, 41
class 2 group, 122, 142
class (conjugacy), 4
class equation, 5
class (nilpotence), 22, 116, 119
class size, 6

- class sizes, common divisor graph, 268
- class sizes, number of, 128
- class sizes, smallest, 128
- classical adjoint of matrix, 321
- collection of commutators, 120*ff*
- common divisor graph on class sizes, 268
- common-divisor graph, components, 265*ff*
- commutator, 40, 48, 113*ff*
- commutator, additive, 125
- commutator collection, 120*ff*
- commutator, multiple, 115
- commutator subgroup, 80 *see also* derived subgroup
- commutators in coprime action, 138
- complement, 85
- complement for normal subgroup, 65
- complete group, 279
- component of group, 273*ff*, 287 *see also* layer
- components of common-divisor graph, 265*ff*
- composition factor, 29
- composition series, 29
- composition series of solvable group, 84
- conjugacy class, 4 *see also* class
- conjugacy of complements, 82
- conjugacy of Sylow subgroups, 14
- conjugates of subgroup, 6
- conjugation action, 2
- conjugation action on normal subgroup, 230
- connected graph, 260
- control of fusion, 158, 167
- control of transfer, 167, 295*ff*
- coprime action, 96*ff*
- coprime action on abelian group, 140
- coprime action, orbit sizes of, 102*ff*
- coprime action, commutators in, 138
- coprime orbit sizes, 102–105
- core of cyclic subgroup, 63
- core, 3
- corefree subgroup, 285
- correspondence theorem, 340
- coset, 331
- coset action, 3
- coset, double, 6, 304
- crossed homomorphism, 76, 114
- cyclic extension, 107
- cyclic factor group, 118
- cyclic group automorphism, 334
- cyclic group, subgroups of, 330
- cyclic subgroup, core of, 63
- cyclic Sylow subgroups, 159*ff*
- derived length, 82
- derived length and nilpotence class, 128
- derived length, large, 146
- derived series, 80
- derived subgroup, 80, 113
- derived subgroup, finiteness, 155
- derived subgroup, noncommutators in, 125
- development, 15
- Dietzmann theorem, 156
- dihedral group, 55*ff*, 120, 189, 196
- dihedral group, construction, 70
- direct diamond, 329
- direct product, 69*ff*
- direct product, center of, 25
- direct product, definition, 342
- Doerk, K., 86
- dot action on right transversal, 148
- double coset, 6, 304
- double transitivity, 225
- E**, 274 *see also* layer
- elementary abelian group, 27, 82, 202, 298, 310
- Euler totient function, φ , 334
- even permutation, 34, 326
- existence of Sylow subgroup, 8, 9, 12
- exponent, 116
- extension, 66
- external direct product, 342
- extraspecial p -group, 123
- F**, 25 *see also* Fitting subgroup
- F***, 271 *see also* generalized Fitting subgroup
- factor group, 337
- faithful action, 2, 40, 133, 233
- faithful action on normal subgroup, 145
- faithful orbit (existence of), 74
- Feit-Thompson theorem, 30, 75, 97
- Feit, W., 30
- finite index center, Schur theorem, 155
- Fischer-Greiss monster, 31
- Fitting subgroup, 25, 46, 53, 271
- Fitting subgroup and subnormality, 47
- Fitting subgroup of solvable group, 86
- Fitting theorem, coprime action, 140
- fixed points come from fixed points, 101
- fixed-point subgroup, 96
- focal subgroup theorem, 165
- Fratini argument, 15
- Fratini subgroup, 27, 95, 282, 330
- Fratini subgroup of p -group, 27, 117
- free abelian group, 315
- Frobenius action, 177*ff*, 232
- Frobenius complement, 26, 179
- Frobenius complement, nonsolvable, 181
- Frobenius complement, odd order, 185, 193
- Dedekind lemma, 328
- degree, 225
- depth, subnormal, 45

- Frobenius complement, properties, 186ff, 193
 Frobenius group, 181
 Frobenius kernel, 179
 Frobenius kernel, nilpotence of, 196ff, 201
 Frobenius kernel, nonabelian, 180
 Frobenius kernel, solvable, 196
 Frobenius p -nilpotence theorem, 171ff, 197
 Frobenius theorem on kernel existence, 181, 186
 Frobenius theorem, permutations, 183
 Frobenius, G., 216
 fundamental counting principle, 5
 Furtwängler, P., 313
 fused classes, 100, 158
 fusion and p -nilpotence, 170
 fusion, control of, 158

 general linear group, 30, 203ff, 228
 general linear group, order of, 204
 general linear group, Sylow subgroup of, 205
 generalized Brodkey theorem, 39
 generalized dihedral group, 57, 70
 generalized Fitting subgroup, 271ff, 276, 281
 generalized quaternion group, 74, 110, 120, 153, 189, 196, 209
 generating set of subgroup, 329
 glasses, 96
 GL , 30 *see also* general linear group
 Glauberman $\mathbf{Z}(J)$ -theorem, 217
 Glauberman lemma, 97
 Glauberman, G., 31, 217
 global property, 59
 Goldschmidt, D., 31, 55, 217
 good theorem, 2
 graph and transpositions, 241
 graph, common divisor, 265ff
 graphs and primitivity, 260
 graphs and orbitals, 259
 greed, 46
 group, definition, 325
 group of order 120, 18, 256
 group of order 21952, 17
 group of order 24, 33
 group of order 8, 190
 group of order p^2q^2 , 37
 group of order p^2q , 32
 group of order p^3q , 33
 group of order p^aq , 37
 group of order pq , 32
 group of order pqr , 38
 group ring, 313
 groups of small order, 38

 half transitivity, 232ff

 Hall C-theorem, 87
 Hall D-theorem, 90
 Hall E-theorem, 86
 Hall E-theorem converse, 87
 Hall π -subgroup, 86
 Hall π -subgroups, nonisomorphic, 90
 Hall subgroup, 12
 Hall subgroup in solvable group, 86
 Hall subgroup in π -separable group, 93
 Hall subgroup, conjugacy, 87
 Hall subgroup, normal, 75
 Hall-Higman Lemma 1.2.3, 93
 Hall-Wielandt transfer theorem, 167, 297
 Hall-Witt identity, 125
 Hall, P., 86, 120, 134
 Hartley-Turull theorem, 102
 Hawkes, T., 86
 Higman, G., 196
 Higman-Sims group, 257
 Hochschild, G., 313
 homomorphism, definition, 337
 homomorphism theorem, 339
 homomorphism, canonical, 338
 Horosevskii theorem, 70
 Huppert theorem on metacyclic Sylows, 308

 imprimitive action, 237
 induced action on factor group, 132
 infinite p -group, 8, 19
 inner automorphism (definition), 335
 internal direct product, 342
 intersection of abelian subgroups, 61
 intersection of subnormal subgroups, 47
 intersection of Sylow subgroups, 37–39
 invariant classes, 100
 invariant cosets, 101
 invariant Sylow subgroups, 96
 involution, 55
 involutions, nonconjugate, 57
 Ishikawa, K., 128
 isomorphism, 333
 Iwasawa lemma, 252

 J, 198 *see also* Thompson subgroup
 Jacobi identity, 125
 Janko group, 164
 join of subgroups, 42
 join of subnormal subgroups, 47ff
 Jordan set, 243
 Jordan theorem, 241ff
 Jordan-Hölder theorem, 29, 84
 Jordan, C., 227

 Kegel, O., 294
 kernel of homomorphism, definition, 338
 kernel of action, 2
 kernel of crossed homomorphism, 76

- kernel of transfer, 165
- Klein group, 34, 46, 56
- Kuo, T., 323
- Lagrange theorem, 331
- Lagrange theorem, converse, 9, 24
- lattice, 42, 47
- layer, 274ff, 282, 287
- left transversal, 77
- Lie ring, 126
- linear representation, 147
- local subgroup, 58
- local subgroup and homomorphism, 59–60
- local-to-global theorem, 59
- lower central series, 116, 127, 281
- lower triangular matrix, 205
- Lucchini theorem, 63
- Lyons, R., 55
- Mackey transfer theorem, 304
- magic eyeglasses, 96
- Mann subgroup, 128
- Manning theorem and 3-transitivity, 264
- Maschke theorem, 309
- Mathieu group, 31, 226ff, 256ff
- matrix unit, 253
- Matsuyama, H., 31, 55, 217
- maximal class p -group, 120
- maximal subgroup, 25, 27
- maximal subgroup, definition, 329
- maximal subgroup of solvable group, 84, 91
- maximal subgroup, nilpotent, 168, 209
- McKay, J., 8
- measure, Chermak-Delgado, 41ff
- metacyclic group, 160, 308ff
- minimal-normal subgroup, 48, 54, 82, 90, 275
- minimal-simple group, 61
- monster simple group, 31
- multiple commutator, 115
- multiple transitivity, 225, 264
- multiple transitivity and primitivity, 240
- N-group, 61
- $n!$ theorem, 4
- Navarro, G., 164
- Neumann, P., 7
- nilpotence and subnormality, 47
- nilpotence class, 22, 116, 119, 296
- nilpotence class and derived length, 128
- nilpotence class of Mann subgroup, 129
- nilpotent factor group, 27
- nilpotent group, 20, 24
- nilpotent injector, 91
- nilpotent joins, Baer theorem, 55
- nilpotent maximal subgroup, 168, 209
- nilpotent normal subgroup, 26
- nonabelian simple group, 29
- normal p -complement, 159, 164
- normal abelian subgroups cyclic, 189
- normal closure, 51
- normal Hall subgroup and splitting, 75
- normal series, 20, 80
- normal subgroup, definition, 336
- normal subgroup of primitive group, 238
- normal-J theorem, 210
- normal- P theorem, 207
- normalizer, 3, 336
- normalizer of subnormal subgroup, 48
- normalizers grow, 22
- O'Brien, E., 19
- odd permutation, 34, 326
- odd-order theorem, 30 *see also* Feit-Thompson theorem
- Ω_r of p -group, 120
- Ω_1 of class 2 p -group, 122
- orbit, 4, 223
- orbit size, 5
- orbits, number of, 7
- orbit sizes in coprime actions, 102
- orbital, 257 *see also* suborbit
- orbits of subgroup, 236
- order of automorphism, 70
- $P \times Q$ -theorem, 139
- $P \times Q$ -theorem, strong form, 144
- $p^a q^b$ theorem, 30, 217ff
- p -central element, 220
- p -complement, 85, 88
- p -complement, normal, 159
- p -cycle in primitive group, 245
- p -group, 8
- p -group of class 2, 122
- p -group of maximal class, 120
- p -group, center of, 20
- p -group, elementary abelian, 27 *see also* elementary abelian
- p -group, infinite, 8
- p -group, nilpotence of, 21
- p -group, omega subgroup of, 120
- p -group, subgroups of, 24
- p -group with unique minimal subgroup, 189
- p -groups, number of, 19
- p -local subgroup, 58
- p -local subgroup of p -solvable group, 140
- p -local subgroups and p -nilpotence, 171
- p -nilpotence and fusion, 170
- p -nilpotent group, 159 *see also* normal p -complement
- p -solvable group, 93, 95, 107, 140, 146, 207, 210
- paired orbital, 257, 262
- partitioned group, 186, 195, 232

- Passman, D., 232, 240
 path connected graph, 260
 perfect group, 151
 permutable subgroups, 6, 49
 permutation character, 7, 236
 permutation group, 223*ff*
 permutation isomorphism, 5, 103, 224
 permutation representation, 2, 223
 Pettet, M., 278
 Φ , 27 *see also* Frattini subgroup
 PGL, 205
 π -group, 12
 π -length, 94
 π -separable group, 91
 π -solvable group, 93
 point stabilizer, 3
 point stabilizer, primitive group, 239
 pointwise stabilizer of set, 242
 Praeger, C., 106, 249, 265, 285
 pretransfer map, 149
 prime degree action, Burnside theorem, 240
 prime index subgroup, 6, 18, 85
 prime order elements central, 174
 prime subdegree, 269
 primitive action, 237*ff*
 primitive group containing p -cycle, 241, 242, 245
 primitive group, simplicity criterion, 252
 primitive solvable group, 248
 primitive subgroup of symmetric group, 246*ff*
 primitivity and multiple transitivity, 240
 principal ideal theorem (of transfer), 313
 pro- p -group, 18
 product of subgroups, 6, 49, 327, 336
 projective general linear group, 205
 projective special linear group, 30 *see also* PSL
 PSL, 30, 205
 PSL, simplicity, 251*ff*

 quasinormal subgroup, 50
 quasisquaternion, 123
 quasisimple group, 272
 quaternion group, 74 *see also* generalized quaternion group
 quotient group, 337

 rank of abelian p -group, 203
 regular p -group, 297, 307
 regular action, 2, 225
 regular orbit, existence, 71
 regular subgroup of permutation group, 235
 regular wreath product, 73
 repeated commutator, 132*ff*
 representation, 147
 representation group (Schur), 151, 272
 representation, permutation, 2
 right transversal, 77
 right transversal, dot action on, 148

 Saxl, J., 249, 285
 Schenkman theorem, 283
 Schenkman, E., 278
 Schur multiplier, 123, 151, 153, 272
 Schur representation group, 151, 272
 Schur theorem, finite index center, 155
 Schur-Zassenhaus theorem, 75*ff*
 second center, 20
 Seitz, G., 249, 285
 self-centralizing subgroup, 129
 self-normalizing Sylow subgroup, 164
 semidihedral group, 74, 120, 189, 196
 semidihedral group, Schur multiplier, 153
 semidirect product, applications of, 70
 semidirect product, existence of, 72
 semiregular action, 177, 225
 semisimple group, 274
 series of subgroups, 20
 setwise stabilizer of set, 242
 sharp multiple transitivity, 226
 sharp transitivity, 225
 simple group, nonabelian, 29
 simple group classification, 30
 simple group, order of, 163
 simple group, Sylow 2-subgroup of, 162
 simple groups of small order, 35
 Sims conjecture, 249, 285
 SL, 30, 110
 SL, order of, 204
 socle, 48, 54
 solvable group, 30, 80*ff*
 solvable group, Fitting subgroup, 86
 solvable group, maximal subgroup, 84
 solvable minimal normal subgroup, 82
 solvable primitive group, 248
 special linear group, 30 *see also* SL
 split extension, 65*ff*
 sporadic simple group, 30
 stabilizer of chain, 137
 stabilizer of point, 3
 strongly conjugate subgroups, 54, 289*ff*
 strongly Jordan set, 243
 subdegree, 259
 subdegrees in imprimitive group, 265
 subdegrees in primitive group, 261*ff*
 subnormal π -subgroup, 53
 subnormal closure, 289*ff*
 subnormal core, 294
 subnormal depth, 45
 subnormal nilpotent subgroup, 47
 subnormal partition, 195
 subnormal series, π -separable, 92
 subnormal subgroup, 45

- subnormality, 45*ff*, 271*ff*
- suborbit, 257*ff*
- supersolvable group, 85
- supersolvable group, Mann subgroup of, 131
- Suzuki, M., 55
- Suzuki group, 163
- Sylow p -subgroup of symmetric group, 299
- Sylow C-theorem, 14
- Sylow counting theorem, 16
- Sylow D-theorem, 15
- Sylow E-theorem, 9
- Sylow subgroup, 8
- Sylow subgroup of Frobenius complement, 188, 193
- Sylow subgroup of general linear group, 205
- Sylow subgroup, cyclic, 159*ff*
- Sylow subgroups, intersection, 10, 16, 38
- Sylow subgroups, number of, 15–16
- Sylow subgroups, set of, 10, 14
- Sylow system, 90
- Sylow theorem, via Cauchy, 8, 12
- symmetric group, 4, 325
- symmetric group automorphism, 250
- symmetric group, normal subgroup of, 251
- symmetric group, primitive subgroup of, 246
- Tate's theorem, 168
- Taussky-Todd, O., 196
- the, 11, 334
- Thompson $P \times Q$ -theorem, 139
- Thompson p -nilpotence theorem, 197, 201, 213
- Thompson subgroup, 198, 201*ff*
- Thompson theorem on Sims conjecture, 285*ff*
- Thompson, J., 30, 61, 169, 217
- Thompson's thesis, 179, 196, 201, 214
- three subgroups lemma, 126
- totient function, 334
- transfer evaluation lemma, 153*ff*
- transfer kernel, 165
- transfer map, 149
- transfer theory, 147*ff*, 295*ff*
- transfer to central subgroup, 154
- transfer to derived subgroup, 313
- transitive action, 7, 223
- transitivity of transfer, 301
- translate of subset in action, 237
- transposition, 240, 326
- transversal, 77 *see also* right transversal
- trivial block, 237
- Verlagerung, 149
- weakly closed subgroup, 163
- weight of commutator, 127
- Weiss theorem on subdegrees, 262
- Wielandt automorphism tower theorem, 278
- Wielandt solvability theorem, 88
- Wielandt subgroup, 54
- Wielandt zipper lemma, 50*ff*
- wreath product, 73, 124, 296
- Yoshida theorem, 296
- Yoshida, T., 167
- Zassenhaus, H., 181
- Zenkov theorem, 61
- zipper lemma, 50
- upper central series, 20
- upper triangular matrix, 204

Titles in This Series

- 97 **David C. Ullrich**, Complex made simple, 2008
- 96 **N. V. Krylov**, Lectures on elliptic and parabolic equations in Sobolev spaces, 2008
- 95 **Leon A. Takhtajan**, Quantum mechanics for mathematicians, 2008
- 94 **James E. Humphreys**, Representations of semisimple Lie algebras in the BGG category \mathcal{O} , 2008
- 93 **Peter W. Michor**, Topics in differential geometry, 2008
- 92 **I. Martin Isaacs**, Finite group theory, 2008
- 91 **Louis Halle Rowen**, Graduate algebra: Noncommutative view, 2008
- 90 **Larry J. Gerstein**, Basic quadratic forms, 2008
- 89 **Anthony Bonato**, A course on the web graph, 2008
- 88 **Nathanial P. Brown and Narutaka Ozawa**, C^* -algebras and finite-dimensional approximations, 2008
- 87 **Srikanth B. Iyengar, Graham J. Leuschke, Anton Leykin, Claudia Miller, Ezra Miller, Anurag K. Singh, and Uli Walther**, Twenty-four hours of local cohomology, 2007
- 86 **Yulij Ilyashenko and Sergei Yakovenko**, Lectures on analytic differential equations, 2007
- 85 **John M. Alongi and Gail S. Nelson**, Recurrence and topology, 2007
- 84 **Charalambos D. Aliprantis and Rabee Tourky**, Cones and duality, 2007
- 83 **Wolfgang Ebeling**, Functions of several complex variables and their singularities (translated by Philip G. Spain), 2007
- 82 **Serge Alinhac and Patrick Gérard**, Pseudo-differential operators and the Nash–Moser theorem (translated by Stephen S. Wilson), 2007
- 81 **V. V. Prasolov**, Elements of homology theory, 2007
- 80 **Davar Khoshnevisan**, Probability, 2007
- 79 **William Stein**, Modular forms, a computational approach (with an appendix by Paul E. Gunnells), 2007
- 78 **Harry Dym**, Linear algebra in action, 2007
- 77 **Bennett Chow, Peng Lu, and Lei Ni**, Hamilton’s Ricci flow, 2006
- 76 **Michael E. Taylor**, Measure theory and integration, 2006
- 75 **Peter D. Miller**, Applied asymptotic analysis, 2006
- 74 **V. V. Prasolov**, Elements of combinatorial and differential topology, 2006
- 73 **Louis Halle Rowen**, Graduate algebra: Commutative view, 2006
- 72 **R. J. Williams**, Introduction the the mathematics of finance, 2006
- 71 **S. P. Novikov and I. A. Taimanov**, Modern geometric structures and fields, 2006
- 70 **Seán Dineen**, Probability theory in finance, 2005
- 69 **Sebastián Montiel and Antonio Ros**, Curves and surfaces, 2005
- 68 **Luis Caffarelli and Sandro Salsa**, A geometric approach to free boundary problems, 2005
- 67 **T.Y. Lam**, Introduction to quadratic forms over fields, 2004
- 66 **Yuli Eidelman, Vitali Milman, and Antonis Tsolomitis**, Functional analysis, An introduction, 2004
- 65 **S. Ramanan**, Global calculus, 2004
- 64 **A. A. Kirillov**, Lectures on the orbit method, 2004
- 63 **Steven Dale Cutkosky**, Resolution of singularities, 2004
- 62 **T. W. Körner**, A companion to analysis: A second first and first second course in analysis, 2004

TITLES IN THIS SERIES

- 61 **Thomas A. Ivey and J. M. Landsberg**, Cartan for beginners: Differential geometry via moving frames and exterior differential systems, 2003
- 60 **Alberto Candel and Lawrence Conlon**, Foliations II, 2003
- 59 **Steven H. Weintraub**, Representation theory of finite groups: algebra and arithmetic, 2003
- 58 **Cédric Villani**, Topics in optimal transportation, 2003
- 57 **Robert Plato**, Concise numerical mathematics, 2003
- 56 **E. B. Vinberg**, A course in algebra, 2003
- 55 **C. Herbert Clemens**, A scrapbook of complex curve theory, second edition, 2003
- 54 **Alexander Barvinok**, A course in convexity, 2002
- 53 **Henryk Iwaniec**, Spectral methods of automorphic forms, 2002
- 52 **Ilka Agricola and Thomas Friedrich**, Global analysis: Differential forms in analysis, geometry and physics, 2002
- 51 **Y. A. Abramovich and C. D. Aliprantis**, Problems in operator theory, 2002
- 50 **Y. A. Abramovich and C. D. Aliprantis**, An invitation to operator theory, 2002
- 49 **John R. Harper**, Secondary cohomology operations, 2002
- 48 **Y. Eliashberg and N. Mishachev**, Introduction to the h -principle, 2002
- 47 **A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi**, Classical and quantum computation, 2002
- 46 **Joseph L. Taylor**, Several complex variables with connections to algebraic geometry and Lie groups, 2002
- 45 **Inder K. Rana**, An introduction to measure and integration, second edition, 2002
- 44 **Jim Agler and John E. McCarthy**, Pick interpolation and Hilbert function spaces, 2002
- 43 **N. V. Krylov**, Introduction to the theory of random processes, 2002
- 42 **Jin Hong and Seok-Jin Kang**, Introduction to quantum groups and crystal bases, 2002
- 41 **Georgi V. Smirnov**, Introduction to the theory of differential inclusions, 2002
- 40 **Robert E. Greene and Steven G. Krantz**, Function theory of one complex variable, third edition, 2006
- 39 **Larry C. Grove**, Classical groups and geometric algebra, 2002
- 38 **Elton P. Hsu**, Stochastic analysis on manifolds, 2002
- 37 **Hershel M. Farkas and Irwin Kra**, Theta constants, Riemann surfaces and the modular group, 2001
- 36 **Martin Schechter**, Principles of functional analysis, second edition, 2002
- 35 **James F. Davis and Paul Kirk**, Lecture notes in algebraic topology, 2001
- 34 **Sigurdur Helgason**, Differential geometry, Lie groups, and symmetric spaces, 2001
- 33 **Dmitri Burago, Yuri Burago, and Sergei Ivanov**, A course in metric geometry, 2001
- 32 **Robert G. Bartle**, A modern theory of integration, 2001
- 31 **Ralf Korn and Elke Korn**, Option pricing and portfolio optimization: Modern methods of financial mathematics, 2001
- 30 **J. C. McConnell and J. C. Robson**, Noncommutative Noetherian rings, 2001
- 29 **Javier Duoandikoetxea**, Fourier analysis, 2001
- 28 **Liviu I. Nicolaescu**, Notes on Seiberg-Witten theory, 2000
- 27 **Thierry Aubin**, A course in differential geometry, 2001
- 26 **Rolf Berndt**, An introduction to symplectic geometry, 2001

For a complete list of titles in this series, visit the
AMS Bookstore at www.ams.org/bookstore/.

The text begins with a review of group actions and Sylow theory. It includes semidirect products, the Schur–Zassenhaus theorem, the theory of commutators, coprime actions on groups, transfer theory, Frobenius groups, primitive and multiply transitive permutation groups, the simplicity of the PSL groups, the generalized Fitting subgroup and also Thompson’s J -subgroup and his normal p -complement theorem.

Topics that seldom (or never) appear in books are also covered. These include subnormality theory, a group-theoretic proof of Burnside’s theorem about groups with order divisible by just two primes, the Wielandt automorphism tower theorem, Yoshida’s transfer theorem, the “principal ideal theorem” of transfer theory and many smaller results that are not very well known.

Proofs often contain original ideas, and they are given in complete detail. In many cases they are simpler than can be found elsewhere. The book is largely based on the author’s lectures, and consequently, the style is friendly and somewhat informal. Finally, the book includes a large collection of problems at disparate levels of difficulty. These should enable students to practice group theory and not just read about it.

Martin Isaacs is professor of mathematics at the University of Wisconsin, Madison. Over the years, he has received many teaching awards and is well known for his inspiring teaching and lecturing. He received the University of Wisconsin Distinguished Teaching Award in 1985, the Benjamin Smith Reynolds Teaching Award in 1989, and the Wisconsin Section MAA Teaching Award in 1993, to name only a few. He was also honored by being the selected MAA Pólya Lecturer in 2003–2005.



Courtesy of D. Finch

ISBN 978-0-8218-4344-4



9 780821 843444

GSM/92



For additional information
and updates on this book, visit

www.ams.org/bookpages/gsm-92

AMS on the Web
www.ams.org